Microwave Data Systems Inc.

MDS *i*NET 900™ Series

Wireless IP/Ethernet Transceiver

Firmware Release 4

MDS 05-2806A01, Rev. E.1
DECEMBER 2005

industrial/wireless/performance

MDS

User's Guide

QUICK-START INSTRUCTIONS

INSTALLATION SUMMARY

Step 1 – Mount the Transceiver

Step 2 – Install the Antenna

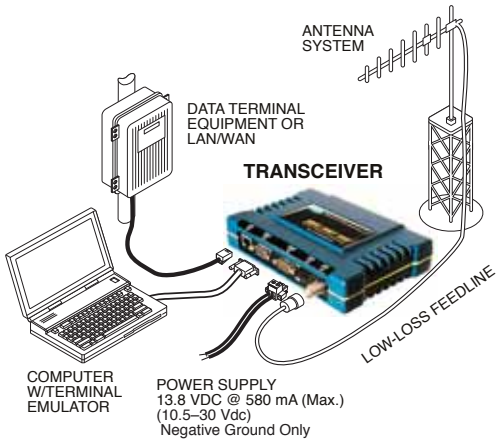
Step 3 – Measure & Connect Primary Power (10.5–30 Vdc)

Step 4 – Review the transceiver's Configuration

Device Mode—Access Point, or Remote (Default)
Network Name—Unique name for each radio network.
Required for Remotes to associate with Access Point.
IP Address—Must be a unique number to allow for IP access through the Ethernet Port.
NOTE: A unique IP address is essential to access the browser-based Management System.
RF Output Power—Adjust as necessary for regulatory compliance. (Default = 1 Watt /+30 dBm)
Password—Used for remote access and some Management System features. (Default = admin)

Step 5 – Connect the Data Equipment

Connect the data equipment to data port(s):
- LAN—10BaseT Ethernet-compatible equipment: Ethernet Hub (Straight-Through Cable); Ethernet Node (Crossover)
- COM2—Serial, RS/EIA-232 compatible equipment
- COM1—Management System (Default); Serial (Alternate)


ANTENNA SYSTEM
DATA TERMINAL EQUIPMENT OR LAN/WAN
TRANSCEIVER
LOW-LOSS FEEDLINE
COMPUTER W/TERMINAL EMULATOR
POWER SUPPLY 13.8 VDC @ 580 mA (Max.) (10.5–30 Vdc) Negative Ground Only

TYPICAL INSTALLATION

Step 6 – Check for Normal Operation

- Observe the transceiver LED status panel for the proper indications. In a normally operating system, the following LED indications will be seen within 30 seconds of power-up:
  PWR—Lights continuously LAN—On or blinks intermittently LINK— On or blinks intermittently (Remotes: if associated)
- Use PING command to test basic data link integrity between Access Point and Remotes.
- If the PING command is successful, connect the RTU/data equipment to the data port and verify normal operation.
- If the LINK LED on Remotes is not on after 20 to 30 seconds, the unit has failed to associate with the Access Point. It may be necessary to reposition or redirect the radio's antenna for better reception/signal strength.
- Check connected data equipment for normal operation

BASIC CONFIGURATION DEFAULTS

The Management System can be accessed through the COM1 Port using a terminal session on a PC. The basic items listed below, along with many other parameters & tools can be accessed through this method. HTTP, Telnet access, and changing some parameters are controlled by password.

ITEM	MGT SYSTEM MENU	DEFAULT	VALUES/RANGE
Device Mode	Network Configuration	Remote	• Remote • Access Point
Unit Password	Device Information	admin (lower case)	• 1–8 alphanumeric characters • Case-sensitive; can be mixed case
Network Name	Network Configuration	"Not Programmed"	• 1–16 alphanumeric characters • Case-sensitive; can be mixed case
IP Address	Network Configuration	192.168.1.1	Contact your Network Administrator
RF Output Power	Radio Configuration	+30 dBm (1.0 Watt)	20–30 dBm @ 50Ω (0.1–1.0 Watt)

Detailed instructions for setting transceiver parameters are contained in Section 3 of this manual.

Contents

1 PRODUCT OVERVIEW AND APPLICATIONS 1

1.1 PRODUCT DESCRIPTION 3

1.1.1 Model Offerings 5

1.2 APPLICATIONS 5

1.2.1 Wireless LAN 5
1.2.2 Point-to-Point LAN Extension 6
1.2.3 Backhaul for Serial Radio Networks 6
1.2.4 Multiple Protocols and/or Services 7
1.2.5 Wireless LAN with Mixed Services 8
1.2.6 Upgrading Older Wireless Network with Serial Interfaces 9
1.2.7 High-Speed Mobile Data 10

1.3 NETWORK DESIGN CONSIDERATIONS 10

1.3.1 Extending Network Coverage with Repeaters 10
1.3.2 Protected Network Operation using Multiple Access Points 12
1.3.3 Collocating Multiple Radio Networks 13

1.4 MDS SECURITY SUITE 14

1.4.1 Early Warning via SNMP Traps 15

1.5 ACCESSORIES 15

2 TABLETOP EVALUATION AND TEST SETUP 17

2.1 OVERVIEW 19

2.2 STEP 1—INSTALL THE ANTENNA CABLING 19

2.3 STEP 2—MEASURE & CONNECT THE PRIMARY POWER 20

2.4 STEP 3—CONNECT PC TO THE TRANSCEIVER 20

2.5 STEP 4—REVIEW TRANSCEIVER CONFIGURATION 21

2.5.1 Getting Started 21
2.5.2 Procedure 21
2.5.3 Basic Configuration Defaults 21

2.6 STEP 5—CONNECT LAN AND/OR SERIAL EQUIPMENT 22

2.7 STEP 6—CHECK FOR NORMAL OPERATION 23

3 EMBEDDED MANAGEMENT SYSTEM 25

3.1 MS INTRODUCTION 27

3.1.1 Differences in the User Interfaces 27

3.2 ACCESSING THE MENU SYSTEM 29

3.2.1 Methods of Control 30
3.2.2 PC Connection & Log In Procedures 30
3.2.3 Navigating the Menus 34

3.3 BASIC DEVICE INFORMATION 36

3.3.1 Starting Information Screen 36
3.3.2 Main Menu 37
3.3.3 Configuring Basic Device Parameters 38

3.4 CONFIGURING NETWORK PARAMETERS 40

3.4.1 Network Configuration Menu 40
3.4.2 IP Address Configuration Menu 42
3.4.3 Ethernet Port Configuration Menu 43
3.4.4 DHCP Server Configuration 44
3.4.5 SNMP Agent Configuration 46

3.5 RADIO CONFIGURATION 48

3.5.1 Radio Configuration Menu 48
3.5.2 Mobile Data Configuration 54

3.6 CONFIGURING THE SERIAL INTERFACES 56

3.6.1 Overview 56
3.6.2 Serial Data Port Configuration Menu 59
3.6.3 Configuring for UDP Mode 60
3.6.4 Configuring for TCP Mode 64
3.6.5 Configuring for PPP Mode 66
3.6.6 IP-to-Serial Application Example 67
3.6.7 Point-to-Point Serial-to-Serial Application Example 68
3.6.8 Point-to-Multipoint Serial-to-Serial Application Example 69
3.6.9 Mixed Modes 71

3.7 SECURITY CONFIGURATION 73

3.7.1 Approved Remotes/Access Points List Menu 75

3.8 PERFORMANCE VERIFICATION 76

3.8.1 Performance Information Menu 76
3.8.2 Network Performance Notes 87

3.9 MAINTENANCE 91

3.9.1 Reprogramming Menu 92
3.9.2 Configuration Scripts Menu 97
3.9.3 Authorization Keys Menu 105
3.9.4 Auto-Upgrade/Remote-Reboot Menu 106
3.9.5 Radio Test Menu 107
3.9.6 Ping Utility Menu 108
3.9.7 Reset to Factory Defaults 108
3.9.8 Resetting the Password 108

4 TROUBLESHOOTING & RADIO MEASUREMENTS 113

4.1 TROUBLESHOOTING 113

4.1.1 Interpreting the Front Panel LEDs 113
4.1.2 Troubleshooting Using the Embedded Management System 114
4.1.3 Using Logged Operation Events 118
4.1.4 Alarm Conditions 118
4.1.5 Correcting Alarm Conditions 120
4.1.6 Logged Events 121

4.2 RADIO (RF) MEASUREMENTS 123

4.2.1 Antenna System SWR and Transmitter Power Output 124
4.2.2 Antenna Aiming 125

5 PLANNING A RADIO NETWORK 129

5.1 INSTALLATION PLANNING 129

5.1.1 General Requirements 129
5.1.2 Site Selection 131
5.1.3 Terrain and Signal Strength 131
5.1.4 Antenna & Feedline Selection 132
5.1.5 How Much Output Power Can be Used? 135
5.1.6 Conducting a Site Survey 135
5.1.7 A Word About Radio Interference 136

5.2 dBm-WATTS-VOLTS CONVERSION CHART 139

6 TECHNICAL REFERENCE 141

6.1 DATA INTERFACE CONNECTORS 143

6.1.1 LAN Port 143
6.1.2 COM1 Port 144
6.1.3 COM2 Port 144

6.2 FUSE REPLACEMENT PROCEDURE 145

6.3 TECHNICAL SPECIFICATIONS 146

6.4 CHANNEL HOP TABLE 149

6.5 SNMP USAGE NOTES 151

6.5.1 Overview 151

7 GLOSSARY OF TERMS & ABBREVIATIONS..... 155

Copyright Notice

This publication is protected by U.S.A. copyright law. Copyright 2005, Microwave Data Systems, Inc. All rights reserved.

ISO 9001 Registration

Microwave Data Systems adheres to the internationally-accepted ISO 9001 quality system standard.

To our Customers

We appreciate your patronage. You are our business. We promise to serve and anticipate your needs. We will strive to give you solutions that are cost effective, innovative, reliable and of the highest quality possible. We promise to build a relationship that is forthright and ethical, one that builds confidence and trust.

What Products are Covered in this Manual?

This manual covers two members of the MDS iNET Transceiver Series, both of which are designed to be operated under the FCC□s Part 15 license-free rules. The standard iNET radio is a Frequency Hopping Spread Spectrum (FHSS) transceiver that operates at data speeds of 256 and 512 kbps.

The iNET II is a similar design, but it does not utilize frequency hopping technology. It operates under the Digital Transmission System (DTS) provisions of Part 15 and can operate at data speeds of 512 or 1024 kbps. Operational differences between these two models are identified, as necessary, in this manual.

Other MDS *i*NET 900 Series Documentation

Installation Guide The associated MDS *i*NET 900 Series Installation Guide, P/N 05-2873A01, is provided with the transceiver and is limited to essential information needed for installers. The installation guide assumes some guidance to installers will be provided by the readers of this manual. This includes such things as antenna selection, radio communication site survey tools and techniques, and network design.

Related Materials on the Internet Data sheets, frequently asked questions, case studies, application notes, firmware upgrades and other updated information is available on the MDS Web site at www.microwavedata.com.

About Microwave Data Systems Inc.

Almost two decades ago, MDS began building radios for business-critical applications. Since then, we've installed more than 500,000 radios in over 110 countries. To succeed, we overcame impassable terrain, brutal operating conditions and disparate, complex network configurations. We also became experts in wireless communication standards and system applications worldwide. The result of our efforts is that today, thousands of utilities around the world rely on MDS-based wireless networks to manage their most critical assets.

The majority of MDS radios deployed since 1985 are still installed and performing within our customers' wireless networks. That's because we design and manufacture our products in-house, according to ISO 9001 which allows us to control and meet stringent global quality standards.

Thanks to our durable products and comprehensive solutions, MDS is the wireless leader in industrial automation including oil and gas production and transportation, water/wastewater treatment, supply and transportation, electric transmission and distribution and many other utility applications. MDS is also at the forefront of wireless communications for private and public infrastructure and online transaction processing. Now is an exciting time for MDS and our customers as we look forward to further demonstrating our abilities in new and emerging markets.

As your wireless needs change you can continue to expect more from MDS. We'll always put the performance of your network above all. Visit us at www.microwavedata.com for more information.

OPERATIONAL & SAFETY NOTICES

RF Exposure

Professional installation required. The radio equipment described in this guide emits radio frequency energy. Although the power level is low, the concentrated energy from a directional antenna may pose a health hazard. Do not allow people to come closer than 23 cm (9 inches) to the antenna when the transmitter is operating in indoor or outdoor environments. More information on RF exposure is on the Internet at www.fcc.gov/oet/info/documents/bulletins.

UL/CSA Notice

This product is available for use in Class 1, Division 2, Groups A, B, C & D Hazardous Locations. Such locations are defined in Article 500 of the National Fire Protection Association (NFPA) publication *NFPA 70*, otherwise known as the National Electrical Code.

The transceiver has been recognized for use in these hazardous locations by two independent agencies Underwriters Laboratories (UL) and the Canadian Standards Association (CSA). The UL certification for the transceiver is as a Recognized Component for use in these hazardous locations, in accordance with UL Standard 1604. The CSA Certification is in accordance with CSA STD C22.2 No. 213-M1987.

UL/CSA Conditions of Approval: The transceiver is not acceptable as a stand-alone unit for use in the hazardous locations described above. It must either be mounted within another piece of equipment which is certified for hazardous locations, or installed within guidelines, or conditions of approval, as set forth by the approving agencies. These conditions of approval are as follows:

The transceiver must be mounted within a separate enclosure which is suitable for the intended application.

The antenna feedline, DC power cable and interface cable must be routed through conduit in accordance with the National Electrical Code.

Installation, operation and maintenance of the transceiver should be in accordance with the transceiver's installation manual, and the National Electrical Code.

Tampering or replacement with non-factory components may adversely affect the safe use of the transceiver in hazardous locations, and may void the approval.

A power connector with screw-type retaining screws as supplied by MDS must be used.

⚠ WARNING

EXPLOSION HAZARD!

Do not disconnect equipment unless power has been switched off or the area is known to be non-hazardous.

Refer to Articles 500 through 502 of the National Electrical Code (NFPA 70) for further information on hazardous locations and approved Division 2 wiring methods.

FCC Part 15 Notices

The transceiver series complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation. This device is specifically designed to be used under Section 15.247 of the FCC Rules and Regulations. Any unauthorized modification or changes to this device without the express approval of Microwave Data Systems may void the user□s authority to operate this device. Furthermore, the iNET Series is intended to be used only when installed in accordance with the instructions outlined in this manual. Failure to comply with these instructions may also void the user□s authority to operate this device.

Part 15 rules also require that the Effective Isotropic Radiated Power (EIRP) from an MDS iNET Series installation not exceed 36 dBm. Refer to *Antenna & Feedline Selection* on Page 132 for more information.

Industry Canada RSS Notices

Operation is subject to the following two conditions: (1) this device may not cause interference, and (2) this device must accept any interference, including interference that may cause undesired operation of the device.

To reduce potential radio interference to other users, the antenna type and its gain should be chosen so that the Equivalent Isotropic Radiated Power (EIRP) is not more than that permitted for successful communication.

This device as been designed to operate with the antennas listed below, and having a maximum gain of 12 dB. Antennas not included in this list or having a gain greater than 12 dB are strictly prohibited for use with this device. The required antenna impedance is 50 ohms. Refer to Table 5-2 on Page 134 for a list of antennas acceptable for use with this transceiver.

Manual Revision and Accuracy

While every reasonable effort has been made to ensure the accuracy of this manual, product improvements may result in minor differences between the manual and the product shipped to you. If you have additional questions or need an exact specification for a product, please contact our Customer Service Team using the information at the back of this guide. In addition, manual updates can often be found on the MDS Web site at www.microwavedata.com.

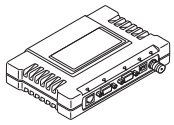
Environmental Information

The manufacture of this equipment has required the extraction and use of natural resources. Improper disposal may contaminate the environment and present a health risk due to hazardous substances contained within. To avoid dissemination of these substances into our environment, and to limit the demand on natural resources, we encourage you to use the appropriate recycling systems for disposal. These systems will reuse or recycle most of the materials found in this equipment in a sound way. Please contact MDS or your supplier for more information on the proper disposal of this equipment.

1 PRODUCT OVERVIEW AND APPLICATIONS

Contents

1.1 PRODUCT DESCRIPTION 3
1.1.1 Model Offerings 5
1.2 APPLICATIONS 5
1.2.1 Wireless LAN 5
1.2.2 Point-to-Point LAN Extension 6
1.2.3 Backhaul for Serial Radio Networks 6
1.2.4 Multiple Protocols and/or Services 7
1.2.5 Wireless LAN with Mixed Services 8
1.2.6 Upgrading Older Wireless Network with Serial Interfaces 9
1.2.7 High-Speed Mobile Data 10
1.3 NETWORK DESIGN CONSIDERATIONS 10
1.3.1 Extending Network Coverage with Repeaters 10
1.3.2 Protected Network Operation using Multiple Access Points 12
1.3.3 Collocating Multiple Radio Networks 13
1.4 MDS SECURITY SUITE 14
1.4.1 Early Warning via SNMP Traps 15
1.5 ACCESSORIES 15



1.1 PRODUCT DESCRIPTION

The MDS *i*NET 900 transceiver provides an easy-to-install wireless solution for local area network (LAN) service with plug-and-play hardware and long range operation. It supports both Ethernet *and* serial data interface options at over-the-air data speeds of up to 512 kbps for *i*NET and 1024 kbps for *i*NET II).

NOTE: For information on the MDS *i*NET 900 ENI, which provides expanded gateway and protocol conversion capabilities not found in the MDS *i*NET 900 (DF1 to EIP, and MODBUS to MODBUS TCP conversions), refer to the MDS *iNET/ENI Supplement* (05-4131A01).

Figure 1-1. The MDS *i*NET 900 Transceiver

Rugged Packaging

The transceiver is housed in a compact and rugged cast-aluminum case that need only be protected from direct exposure to the weather. It contains a single printed circuit board with all necessary components for radio operation and data communications. The only user-serviceable component inside the case is a fuse on the DC power input line.

Simple Installation

Most installations employ an omni-directional antenna at the Access Point (AP) location and a directional antenna at each Remote unit. The antenna is a vital link in the system and must be chosen and installed correctly. Consult *INSTALLATION PLANNING* on Page 129 for guidance on choosing suitable installation sites and antennas.

For basic services, simply connect an antenna, connect your Ethernet LAN to the transceiver's LAN port, apply primary power, set a few operating parameters, and you are done. No license is required for operation in the U.S.A., Canada, and many other countries. Check requirements for your region before placing the transceiver in service.

Secure Operation

Data network security is a vital issue in today's wireless world. The MDS *i*NET 900 Series design provides multiple tools to help you build a network that minimizes the risk of eavesdropping and unauthorized access. Some are inherent in the radio's operation, such as the use of spread-spectrum transmissions; others include data encryption, en-

abling/disabling remote access channels, and password protection.

Remember, security is not a one-step process that can simply be turned on and forgotten. It must be practiced and enforced at multiple levels, 24 hours-a-day and 7 days-a-week. See *"MDS SECURITY SUITE"* on Page 14 for more information about the transceiver's security tools.

Robust Radio Operation

The transceiver is designed for frequency-hopping spread-spectrum operation (DTS for *i*NET II) in the license-free 900 MHz Industrial, Scientific, and Medical (ISM) band. It can provide reliable communications at distances up to 25 miles (40 km) over favorable terrain, even in the presence of weak signals or interference.

Flexible Services

Users with a mixture of equipment having Ethernet and serial data interfaces can choose to use one or two of the user-configurable serial ports through the use of a Remote Dual Gateway. This flexibility allows the transceiver to provide services in data networks that are being migrated from legacy serial/EIA-232-based hardware to the faster and more easily interfaced Ethernet world.

Flexible Management

Configuration, commissioning, troubleshooting and other maintenance activities can be done locally or remotely. Four different modes of access are available: local RS-232 console, local or remote IP access (via Telnet), web browser, and SNMP (v1/v2/v3). The text-based interface (RS-232 console and Telnet) is implemented in the form of easy-to-follow menus, and the terminal server configuration includes a wizard to help you set up the units correctly.

Transceiver Features

The transceiver's design makes the installation and configuration easy, while allowing for changes in the future.

- Long Range—Up to 25 miles (40 km) in line-of-sight conditions. Repeater stations may be used to extend the operational range. (Refer to *TECHNICAL SPECIFICATIONS* on Page 146 for more detailed information on range.)
- Industrial-Grade Product—Extended temperature range for trouble-free operation in extreme environments
- Robust Radio Communications—Designed to operate in dense, high-interference environments
- Robust Network Security—Prevents common attack schemes and hardware from gaining access or control of network. Common attack events logged and reported by alarms.
- High Speed—512 kbps is 50-times faster than 9.6 kbps radios
- Plug-and-Play Connectivity—Ethernet bridge configuration option requires minimal setup
- Serial Ports—Gateway for serial-based equipment to IP/Ethernet networks with embedded terminal server. Site-to-site configurations are also possible.
- Single hardware package provides configuration as Access Point or Remote

1.1.1 Model Offerings

The transceiver comes in two primary models—Access Point and Remote. Three types of Remote Gateways are available—the Ethernet Bridge, the Serial Gateway, and the Dual Gateway supporting both IP/Ethernet and serial services. Table 1-1 summaries the different interface abilities for each type.

A unit can be configured by the owner to operate as an Access Point or as a Remote with some restrictions. Only the Dual Gateway Remote units can be reconfigured as an Access Point. Ethernet Bridge and a Serial Gateway Remotes cannot be reconfigured as Access Point unless they are first upgraded to Dual Gateway type. This is accomplished with an "Authorization Key" purchased from the factory. Each one of these individual software keys is associated with the serial number of the corresponding unit.

Table 1-1. Transceiver Models and Data Interface Services

Model	Type	LAN[1]	COM1[1]	COM2
Access Point[3]	N/A	Yes	Yes	Yes
Remote…	Ethernet Bridge[2]	Yes	No	No
	Serial Gateway[2]	No	Yes	Yes
	Dual Gateway[3]	Yes	Yes	Yes

NOTES
1. Provides access to the embedded Management System on all units.
2. Can be upgraded to Dual Gateway with an Authorization Key.
3. Can be configured as an Access Point or Dual Gateway through the embedded Management System.
4. In addition, the *i*NET II is available. This model operates at 512/1024 kbps under the FCC DTS rules, which allow wider modulation bandwidths to be employed.

1.2 APPLICATIONS

The following sections provide illustrations of typical transceiver installations. This is meant as an overview only. It is recommended that a network manager be involved in all installation planning activities.

1.2.1 Wireless LAN

The wireless LAN is the most common application of the transceiver. It consists of a central control station (Access Point) and one or more associated Remote units, as shown in Figure 1-2 on Page 6. A LAN provides communications between a central WAN/LAN and remote Ethernet segments. The operation of the radio system is transparent to the computer equipment connected to the transceiver.

The Access Point is positioned at a location from which it can communicate with all of the Remote units in the system. Commonly, this is a high location on top of a building or communications tower. Messages are exchanged at the Ethernet level. This includes all types of IP traffic.

A Remote transceiver can only talk over-the-air to an Access Point unit (AP). Peer-to-peer communications between Remotes can only take place indirectly via the AP. In the same fashion, an AP can only talk over-the-air to associated Remote units. Exception: Two APs can communicate with each other "off-the-air" through their Ethernet connectors using a common LAN/WAN.

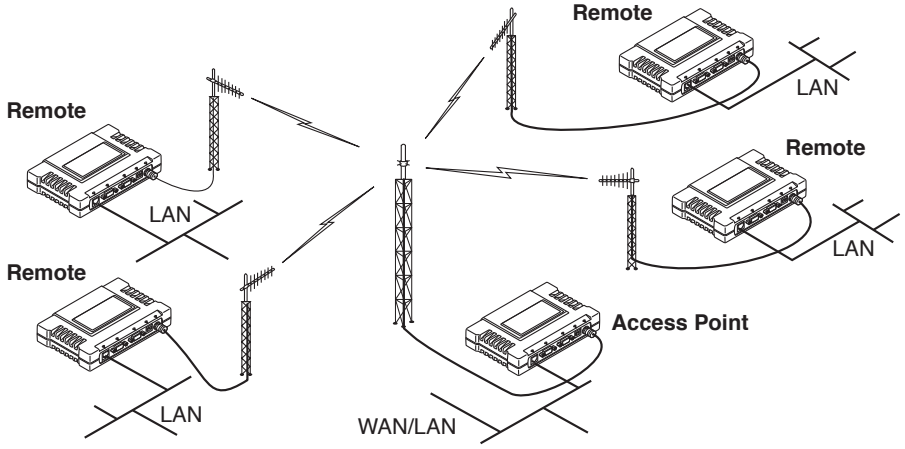


Figure 1-2. Typical Wireless LAN

1.2.2 Point-to-Point LAN Extension

A point-to-point configuration (Figure 1-3) is a simple arrangement consisting of an Access Point and a Remote unit. This provides a communications link for the transfer of data between two locations.

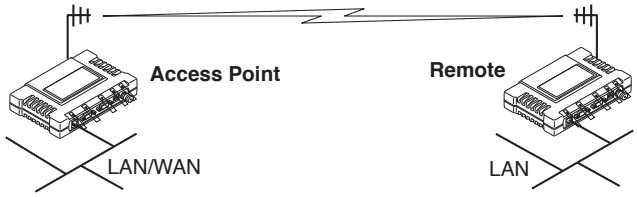


Figure 1-3. Typical Point-to-Point Link

1.2.3 Backhaul for Serial Radio Networks

One of the primary design features of the transceiver is to provide a path for serial devices to migrate to IP/Ethernet. Many radio networks in operation today still rely on serial networks at data rates of 9600 bps or less. These networks can use the transceiver as a means to continue using the serial service, while allowing the rest of the infrastructure to migrate to an IP format.

A Remote transceiver using one serial port for the data stream, and the other for network-wide diagnostics can support operational radio networks built with earlier MDS radios, such as MDS x790/x710, MDS x810 and others. In the case of these existing radios, where a single port is used for data and diagnostics, the capabilities are doubled. The data streams are delivered to an IP socket in an application, or in serial format using the Access Point.

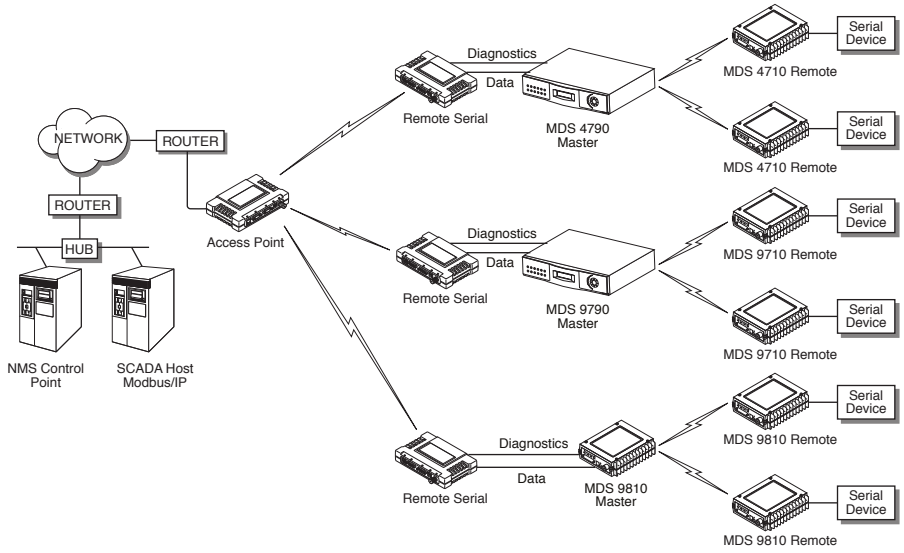


Figure 1-4. Backhaul Network

1.2.4 Multiple Protocols and/or Services

Prior to the MDS 900 Series, two radios were often used to service two different types of devices (typically connected to different SCADA hosts). An *i*NET 900 radio provides this functionality with a single remote radio. Each of the two serial ports can be connected via IP to different SCADA hosts, transporting different (or the same) protocols. Both data streams are completely independent and the transceiver provides seamless simultaneous operation as shown in Figure 1-5 on Page 8.

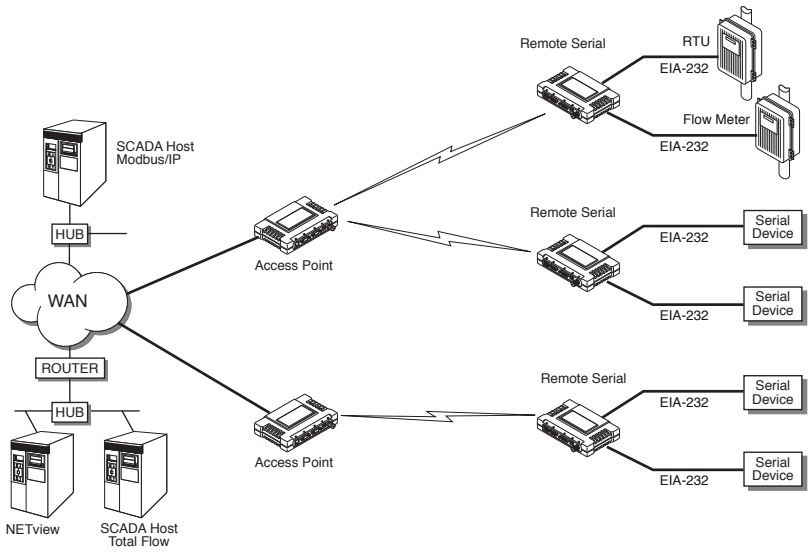


Figure 1-5. Multiple Protocol Network

By using a single radio, the cost of deployment is cut in half. Beyond requiring only one radio instead of two, the biggest cost reduction comes from using half of the required infrastructure at the remote site: one antenna, one feedline, one lightning protector and ancillary hardware. Other cost reductions come from the system as a whole, such as reduced management requirements. And above all, the potential for future applications that run over Ethernet and IP, such as video for remote surveillance.

1.2.5 Wireless LAN with Mixed Services

The transceiver is an excellent solution for a long-range industrial wireless LAN. It offers several advantages over commercial solutions—primarily improved performance over extended distances. The rugged construction of the radio and its extended temperature range make it an ideal solution even in harsh locations. In extreme environments, a simple NEMA enclosure is sufficient to house the unit.

The transceiver trades higher speed for longer range. Commercial 802.11b solutions are designed to provide service to relatively small areas such as offices, warehouses and homes. They provide high data rates but have limited range. The *i*NET 900 transmits at a higher power level, uses a different frequency band, has higher sensitivity, and a narrower channel to concentrate the radio energy and reach farther distances. It is designed for industrial operation from the ground up.

IP-based devices that may be used with the transceiver include a new breed of more powerful Remote Terminal Units (RTUs) and Programmable Logic Controllers (PLCs). These, as well as other devices, may be used in applications ranging from SCADA/telemetry monitoring, web-based video, security monitoring, and voice over IP. Figure 1-6 shows a typical wireless IP network.

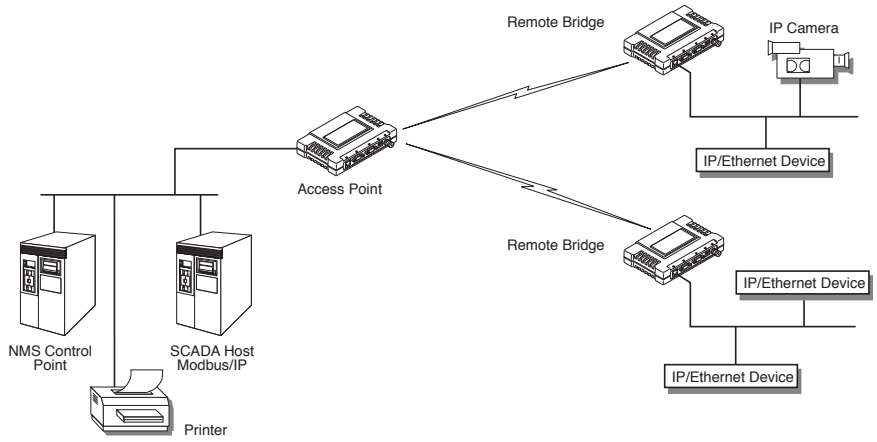


Figure 1-6. Extended-Range LAN with Mixed Applications

1.2.6 Upgrading Older Wireless Network with Serial Interfaces

Millions of wireless data products have been sold in the last two decades for licensed and license-free operation, many of them manufactured by Microwave Data Systems. There are several ways that these systems can benefit from incorporating MDS *i*NET 900 equipment. The chief advantages are interface flexibility (serial and Ethernet in one unit), and higher data throughput. By taking advantage of its built-in serial and Ethernet interfaces, the transceiver is well suited to replace leased lines, dial-up lines, or existing 900 MHz data transceivers.

Replacing Legacy Wireless Products

In most cases, legacy radio transceivers supporting serial-interface equipment can be replaced with *i*NET 900 transceivers. Legacy equipment can be connected to the transceiver through the COM1 or COM2 port with a DB-25 to DB-9 cable wired for EIA-232 signaling. The COM2 port supports all standard EIA-232 signaling and acts as a data-terminal equipment device (DTE).

NOTE: Several previous MDS-brand products had non-standard signal lines on their interface connectors (for example, to control sleep functions and alarm lines). These special functions are not provided nor supported by the *i*NET transceiver. Consult equipment manuals for complete pinout information.

Supplement legacy wireless network with IP services

The MDS *i*NET 900 Dual Gateway model can support up to two serial devices and one Ethernet connection at the same time. The serial interfaces (COM1 and COM2) operate in two different modes: Connectionless UDP and connection-orientated TCP.

In the UDP mode, the transceiver supports point-to-multipoint serial-port to serial-port connectivity. In the TCP mode, it supports point-to-point Ethernet/IP to serial port connectivity.

For further details on the transceiver's Serial Gateway interface modes, see *"CONFIGURING THE SERIAL INTERFACES"* on Page 56.

1.2.7 High-Speed Mobile Data

The *i*NET radios support high-speed data communications in a mobile environment. Remote radios roam between different access points, providing seamless transitions and continuous coverage. For additional information on configuring a mobile network, refer to *Mobile Data Configuration* on Page 54.

1.3 NETWORK DESIGN CONSIDERATIONS

1.3.1 Extending Network Coverage with Repeaters

What is a Repeater System?

A repeater works by re-transmitting data from outlying remote sites to the Access Point and vice-versa. It introduces some additional end-to-end transmission delay but provides longer-range connectivity.

In some geographical areas, obstacles can make communications difficult. These obstacles are commonly large buildings, hills, or dense foliage. These obstacles can often be overcome with a repeater station.

Option 1—Using two transceivers to form a repeater station (back-to-back repeater)

Although the range between transceivers can be up to 40 km (25 miles) over favorable terrain, it is possible to extend the range considerably by connecting two units together at one site in a "back-to-back" fashion to form a repeater, as shown in Figure 1-7. This arrangement should be used whenever the objective is to utilize the maximum range between stations. In this case, using high-gain Yagi antennas at each location will provide more reliable communications than their counterparts—omni-directional antennas.

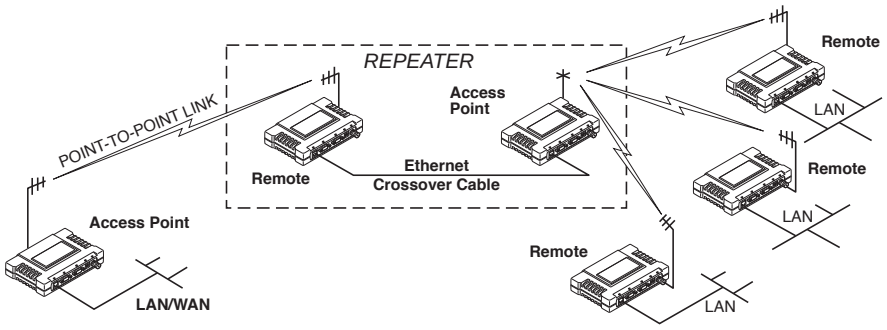


Figure 1-7. Typical LAN with a Repeater Link

Overview

Two transceivers may be connected "back-to-back" through the LAN Ports to form a repeater station. (The cable must be a "cross-over" Ethernet cable for this to work). This configuration is sometimes required in a network that includes a distant Remote that would otherwise be unable to communicate directly with the Access Point station due to distance or terrain.

The geographic location of a repeater station is especially important. A site must be chosen that allows good communication with *both* the Access Point and the outlying Remote site. This is often on top of a hill, building, or other elevated terrain from which both sites can be "seen" by the repeater station antennas. A detailed discussion on the effects of terrain is given in Section 5.1.2, *Site Selection* (beginning on Page 131).

The following paragraphs contain specific requirements for repeater systems.

Antennas

Two antennas are required at this type of repeater station—one for each radio. Measures must be taken to minimize the chance of interference between these antennas. One effective technique for limiting interference is to employ *vertical separation*. In this arrangement, assuming both are vertically polarized, one antenna is mounted *directly* over the other, separated by at least 10 feet (3 Meters). This takes advantage of the minimal radiation exhibited by most antennas directly above and below their driven elements.

Another interference reduction technique is to cross-polarize the repeater antennas. If one antenna is mounted for polarization in the vertical plane, and the other in the horizontal plane, an additional 20 dB of attenuation can be achieved. (Remember that the corresponding stations should use the same antenna orientation when cross-polarization is used.)

Network Name

The two radios that are wired together at the repeater site *must* have different network names. To set or view the network names, see *"STEP 3—CONNECT PC TO THE TRANSCEIVER"* on Page 20 for details.

Option 2—Using the AP as a Store-and-Forward Packet Repeater

A wireless network can be extended through the use of an alternate arrangement using the Access Point as a repeater to re-transmit the signals of all stations in the network. The repeater is a standard transceiver configured as an Access Point, and operating in Store and Forward mode. (See Figure 1-8.)

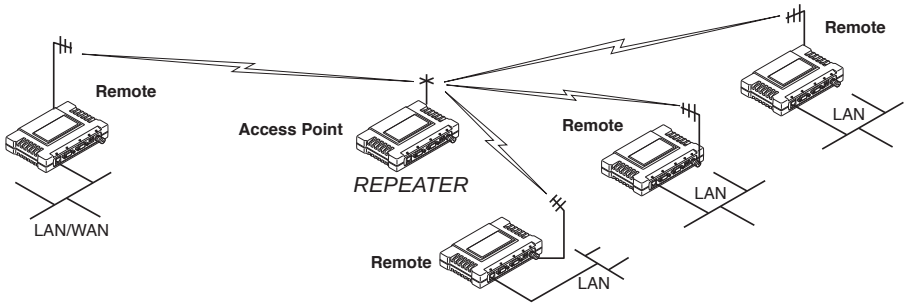


Figure 1-8. Typical network with store-and-forward repeater

As with the conventional repeater described in Option 1 above, the location of a store and forward repeater is also important. A site must be chosen that allows good communication with *both* the Access Point and the outlying Remote site. This can be on the top of a hill, building, or other elevated terrain from which all sites can be "seen" by the repeater station antenna. A detailed discussion on the effects of terrain is given in Section 5.1.2, *Site Selection* (beginning on Page 131)

1.3.2 Protected Network Operation using Multiple Access Points

Although MDS transceivers have a very robust design and have undergone intensive testing before being shipped, it is possible for isolated failures to occur. In mission-critical applications, down time can be virtually eliminated by using some, or all, of the following configurations:

In a point-to-multipoint scenario, the Access Point services multiple remotes. A problem in the Access Point will have an effect on all remotes, since none will have access to the network. When operation of the network does not tolerate any down time, it is possible to set up a protected configuration for the Access Point to greatly reduce the possibility of this occurrence.

Two or more Access Points can be configured with the same Network Name and kept active simultaneously, each with its own independent antenna. In this scenario, Remotes will associate with either one of the available Access Points. In case of a failure of one of the AP's the Remotes will quickly associate with another of the remaining Access Points re-establishing connectivity to the end devices.

The Access Points are unaware of the existence of the other AP's. Because the hopping algorithm uses *both* the Network Name *and* the Wireless MAC address of the AP to generate the hopping pattern, multiple AP's can coexist—even if they use the same network name. The collocated AP's will be using different hopping patterns and frequencies the great majority of the time. Although some data collisions will occur, the wireless-MAC is built to tolerate and recover from such occurrences with minimal degradation.

1.3.3 Collocating Multiple Radio Networks

Many networks can operate in relatively close physical proximity to one another provided reasonable measures are taken to assure the radio signal of one Access Point is not directed at the antenna of the second Access Point**.**

The Network Name and the association process

The Network Name is the foundation for building individual radio networks. It is part of a beacon signal broadcast by the Access Point (AP) to any Remote units with the same Network Name. Remotes that join the network are referred to as being "associated" with the Access Point unit.

Multiple APs with the same Network Name should be avoided unless a redundant system is being deployed. Using the same Network Name in multiple APs may result in Remotes associating with undesired APs and preventing data exchange from occurring.

The use of a different Network Name does not guarantee an interference-free system. It does however, assure that only data destined for a unique network is passed through to that network.

Co-Location for Multiple Networks

It may be desirable to co-locate Access Points at one location to take advantage of an excellent or premium location that can serve two independent networks. Each network should have unique Network Name and each AP unit's antenna should be provided as much vertical separation as is practical to minimize RFI.

NOTE: All transceivers are shipped with the Network Name set to "Not Programmed." The Network Name must be programmed in order to pass data and begin normal operations.

Can radio frequency interference (RFI) disrupt my wireless network?

When multiple radio networks operate in close physical proximity to other wireless networks, individual units may not operate reliably under weak signal conditions and may be influenced by strong radio signals in adjacent bands. This radio frequency interference cannot be predicted with certainty, and can only be determined by experimentation. If you need to co-locate two units, start by using the largest possible vertical

antenna separation between the two AP antennas on the same support structure. If that does not work, consult with your factory representative about other techniques for controlling radio frequency interference between the radios. (See *"A Word About Radio Interference"* on Page 136 for more details.)

1.4 MDS SECURITY SUITE

Today the operation and management of an enterprise is becoming increasing dependent on electronic information flow. An accompanying concern becomes the security of the communication infrastructure and the security of the data itself.

The MDS *i*NET 900 transceiver is capable of dealing with many common security issues. Table 1-2 profiles security risks and how the transceiver provides a solution for minimizing vulnerability.

Table 1-2. Security Risk Management

Security Vulnerability	MDS *i*NET 900 Solution
Unauthorized access to the backbone network through a foreign remote radio	• Approved Remotes List Only those remotes included in the AP list will associate
"Rogue" AP, where a foreign AP takes control of some or all remote radios and thus remote devices	• Approved AP List A remote will only associate to those AP included in its local authorized list of AP
Dictionary attacks, where a hacker runs a program that sequentially tries to break a password.	• Failed-login lockdown After 3 tries, the transceiver ignores login requests for 5 minutes. Critical event reports (traps) are generated as well.
Denial of service, where Remote radios could be reconfigured with bad parameters bringing the network down.	•Remote login •Local console login •Disabled HTTP & Telnet to allow only local management services
Airsnort and other war-driving hackers in parking lots, etc.	•900 MHz FHSS for *i*NET (DTS for *i*NET II) does not talk over the air with standard 802.11b cards •The transceiver cannot be put in a promiscuous mode •Proprietary data framing
Eavesdropping, intercepting messages	•128-bit encryption
Key cracking	• Automatic Rotating Key algorithm
Replaying messages	•128-bit encryption with rotating keys

Table 1-2. Security Risk Management

Security Vulnerability	MDS *i*NET 900 Solution
Unprotected access to configuration via SNMPv1	• Implement SNMPv3 secure operation
Intrusion detection	• Provides early warning via SNMP through critical event reports (unauthorized, logging attempts, etc.)

1.4.1 Early Warning via SNMP Traps

In addition to the operative tools and techniques, the transceiver can send SNMP traps (alarms) to a network management systems when certain potentially suspicious activities or events occur. The alarms include:

- Unauthorized AP MAC address detected at Remote
- Unauthorized Remote MAC address detected at AP
- Login attempt limit exceeded
  (Accessed via: Telnet, HTTP, or local)
- Successful login/logout
  (Accessed via: Telnet, HTTP, or local)

1.5 ACCESSORIES

The transceiver can be used with one or more of the accessories listed in Table 1-3. Contact the factory for ordering details.

Table 1-3. Accessories

Accessory	Description	MDS Part No.
AC Power Adapter Kit	A small power supply module designed for continuous service. UL approved. Input: 120/220; Output: 13.8 Vdc @ 2.5 A	01-3682A02
Omni-Directional Antennas	Rugged antennas well suited for use at Access Point installations. Consult with your factory Sales Representative for details	Call factory
Yagi Antenna (Directional)	Rugged antennas well suited for use at Remote installations. Consult with your factory Sales Representative for details.	Call factory
TNC Male-to-N Female Adapter	One-piece RF adaptor plug.	97-1677A161
TNC Male-to-N Female Adapter Cable	Short length of coaxial cable used to connect the radio's TNC antenna connector to a Type N commonly used on large diameter coaxial cables.	97-1677A159 (3 ft./1m) 97-1677A160 (6 ft./1.8m)
Ethernet RJ-45 Crossover Cable (CAT5)	Cable assembly used to cross-connect the Ethernet ports of two transceivers used in a repeater configuration. (Cable length ≈ 3 ft./1M)	97-1870A21

Table 1-3. Accessories

Accessory	Description	MDS Part No.
2-Pin Power Plug	Mates with power connector on transceiver. Screw terminals provided for wires, threaded locking screws to prevent accidental disconnect.	73-1194A39
Ethernet RJ-45 Straight-thru Cable (CAT5)	Cable assembly used to connect an Ethernet device to the transceiver. Both ends of the cable are wired identically. (Cable length ≈ 3 ft./1M)	97-1870A20
EIA-232 Shielded Data Cable	Shielded cable terminated with a DB-25 male connector on one end, and a DB-9 female on the other end. Two lengths available (see part numbers at right).	97-3035L06 (6 ft./1.8m) 97-3035L15 (15 ft./4.6m)
EIA-232 Shielded Data Cable	Shielded cable terminated with a DB-9 male connector on one end, and a DB-9 female on the other end, 6 ft./1.8m long.	97-1971A03
Fuse	Small, board-mounted fuse used to protect against over-current conditions.	29-1784A03
Flat-Surface Mounting Brackets & Screws	Brackets: 2″ x 3″ plates designed to be screwed onto the bottom of the unit for surface-mounting the radio.	82-1753-A01
	Screws: 6-32/1/4″ with locking adhesive. (Industry Standard MS 51957-26)	70-2620-A01
DIN Rail Mounting Bracket	Bracket used to mount the transceiver to standard 35 mm DIN rails commonly found in equipment cabinets and panels.	03-4022A02
COM2 Interface Adapter	DB-25(F) to DB-9(M) shielded cable assembly (6 ft./1.8 m) for connection of equipment or other EIA-232 serial devices previously connected to “legacy” units. (Consult factory for other lengths and variations.)	97-3035A06
MDS NETview MS Software	PC-based network management system for new-generation MDS transceivers. Allows radio control and diagnostics in a hierarchal map perspective.	03-3938A01
Bandpass Filter	Antenna system filter that helps eliminate interference from nearby paging transmitters.	20-2822A02
Ethernet Surge Suppressor	Surge suppressor for protection of Ethernet port against lightning. 10/100BaseT compatible.	29-4018A01

2 TABLETOP EVALUATION AND TEST SETUP

Contents

2.1 OVERVIEW 19

2.2 STEP 1—INSTALL THE ANTENNA CABLING 19

2.3 STEP 2—MEASURE & CONNECT THE PRIMARY POWER . 20

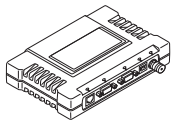
2.4 STEP 3—CONNECT PC TO THE TRANSCEIVER 20

2.5 STEP 4—REVIEW TRANSCEIVER CONFIGURATION 21

2.5.1 Getting Started 21
2.5.2 Procedure 21
2.5.3 Basic Configuration Defaults 21

2.6 STEP 5—CONNECT LAN AND/OR SERIAL EQUIPMENT 22

2.7 STEP 6—CHECK FOR NORMAL OPERATION 23



2.1 OVERVIEW

It is best to set up a tabletop network that can be used to verify the basic operation of the transceivers and give you a chance to experiment with network designs, configurations or network equipment in a convenient location. This test can be performed with any number of radios.

When you are satisfied that the network is functioning properly in a bench setting, field installation can be performed. Complete information for field installation, including mounting dimensions and antenna selection, is provided in *INSTALLATION PLANNING* on Page 129

For the following evaluation, one of the transceivers in the network must be set to Access Point service (**Device Mode = Access Point**) for proper operation.

NOTE: It is important to use a "Network Name" that is different from any currently in use in your area during the testing period. This will eliminate unnecessary disruption of traffic on the existing network while you become familiar with the transceiver or evaluate variations of unit operating parameters.

To simulate data traffic over the radio network, connect a PC or LAN to the Ethernet port of the Access Point and PING each *transceiver* several times.

2.2 STEP 1—INSTALL THE ANTENNA CABLING

Figure 2-1 is a drawing of the tabletop arrangement. Connect the antenna ports of each transceiver as shown. This will provide stable radio communications between each unit while preventing interference to nearby electronic equipment from a large number of co-located units.

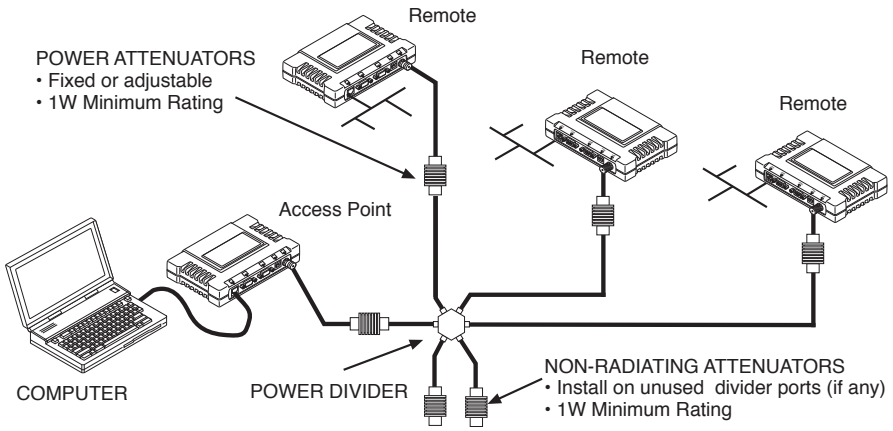


Figure 2-1. Typical setup for tabletop-testing of radios

NOTE: It is very important to use attenuation between all units in the test setup. The amount of attenuation required will depend on the number of units being tested and the desired signal strength (RSSI) at each transceiver during the test. In no case should a signal greater than –50 dBm be applied to any transceiver in the test setup. An RF power output level of +20 dBm is recommended. (See *"Radio Configuration Menu"* on Page 48.)

2.3 STEP 2—MEASURE & CONNECT THE PRIMARY POWER

The primary power at the transceiver's power connector must be within 10–30 Vdc and be capable of continuously providing a minimum of 8 Watts (typical power consumptions are: 760 mA @ 10.5 Vdc, 580 mA @ 13.8 Vdc, and 267 mA @ 30 Vdc).

A power connector with screw-terminals is provided with each unit. Strip the wire leads to 6 mm (0.25"). Be sure to observe proper polarity as shown in Figure 2-2 with the positive lead (+) on the left.

NOTE: It will take about 30 seconds for the transceiver to power up and be ready for operation.

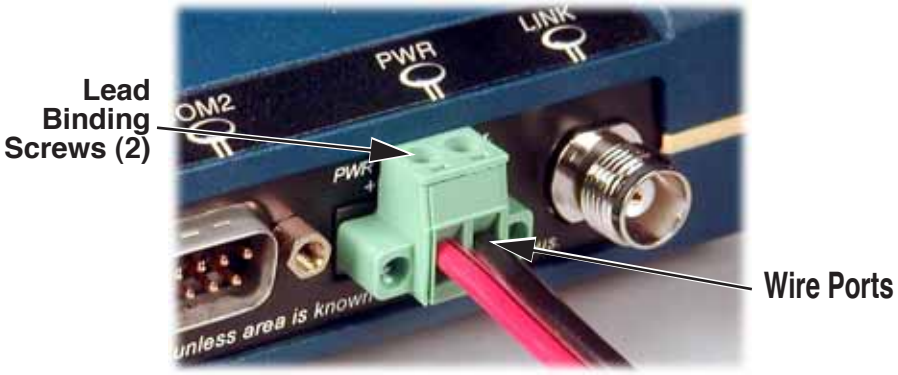


Figure 2-2. Power Connector, Polarity: Left +, Right –

CAUTION
POSSIBLE EQUIPMENT DAMAGE

The transceiver must only be used with negative-ground systems. Make sure the polarity of the power source is correct. The unit is protected from reverse polarity by an internal diode and fuse.

2.4 STEP 3—CONNECT PC TO THE TRANSCEIVER

Connect a PC's Ethernet port to the LAN port using an Ethernet cross-over cable. The LAN LED should light. Alternately, you can use a serial cable to connect to the COM1 port. (Figure 2-3 on Page 23)

2.5 STEP 4—REVIEW TRANSCEIVER CONFIGURATION

2.5.1 Getting Started

Start by logging into the Access Point. Set up the Access Point first because the Remotes are dependent on its beacon signal to achieve the "associated" state.

NOTE: Transceivers are shipped from the factory set to the "Remote" mode unless they are marked differently.

Once the Access Point is up and running, move the computer connection to each of the Remote units, log-in at each unit, review their configuration, set their IP addresses and Network Name and wait for each to achieve the associated state.

With all units associated, you will be ready to connect and test your data services.

2.5.2 Procedure

The following is a summary of the configuration procedure that must be done on each unit in the system. Key parameters are shown on the Embedded Management System overview (Figure 3-1 on Page 28). A lists of parameters can found in two tables: Table 4-5 on Page 119 and Table 4-7 on Page 122. Detailed information on using the Management System can be found in *MS INTRODUCTION* on Page 27.

NOTE: The Management System supports the use of "configuration files" to aid in uniformly configuring multiple units. These are detailed in *Using Configuration Scripts* on Page 98.

2.5.3 Basic Configuration Defaults

Table 2-1 provides a selection of key operating parameters, their range, and default values. All of these are accessible through a terminal emulator connected to the COM1 serial port or through a Web browser connected to the LAN Port. (See Figure 5-1 on Page 129 for hookup.)

NOTE: Access to the transceiver's Management System and changes to some parameters, are controlled by password when accessing by means of a Web browser or Telnet.

Table 2-1. Basic Configuration Defaults

Item	Menu Location	Default	Values/Range
Device Mode[1]	Main Menu>> Network Configuration>> Device Mode	Marked on unit's ID label	• Access Point • Dual Remote • Serial Gateway • Ethernet Bridge
Network Name	Main Menu>> Network Configuration>> Network Name	"Not Programmed"	• 1–15 alphanumeric characters • Case-sensitive; can be mixed case
IP Address	Main Menu>> Network Configuration>> IP Address	192.168.1.1	Contact your network administrator
RF Output Power	Main Menu>> Radio Configuration>> RF Output Power	30 dBm (1.0 Watt)	20–30 dBm @ 50Ω (0.1–1.0 Watts)
Unit Password	Main Menu>> Device Information>> User Password	admin (lower case)	• 1–8 alphanumeric characters • Case-sensitive; can be mixed case

1. Ethernet Bridge and Serial Gateway will not be displayed if a superior mode is authorized for this unit.

A unique IP address and subnet are required to access the browser-based Management System either through the LAN port, or remotely over-the-air.

2.6 STEP 5—CONNECT LAN AND/OR SERIAL EQUIPMENT

Connect a local area network to the LAN port or serial devices to the COM1 (DCE) or COM2 (DTE) ports. Make sure your transceivers are capable of supporting your devices. (See *Table 1-1 . Transceiver Models and Data Interface Services*, on page 5 for a summary of model capabilities.) The LAN port will support any Ethernet-compatible equipment. This includes devices that use the Internet Protocol (IP).

NOTE: If you configure COM1 for payload data service while you are plugged into it, you will not be able to access the management system. Alternate methods for accessing the management system are: use Telnet or the web browser through the Ethernet port; use Telnet or the web browser through the antenna port (remote management).

Figure 2-3 on Page 23 shows the default functions and services for the interface connectors.

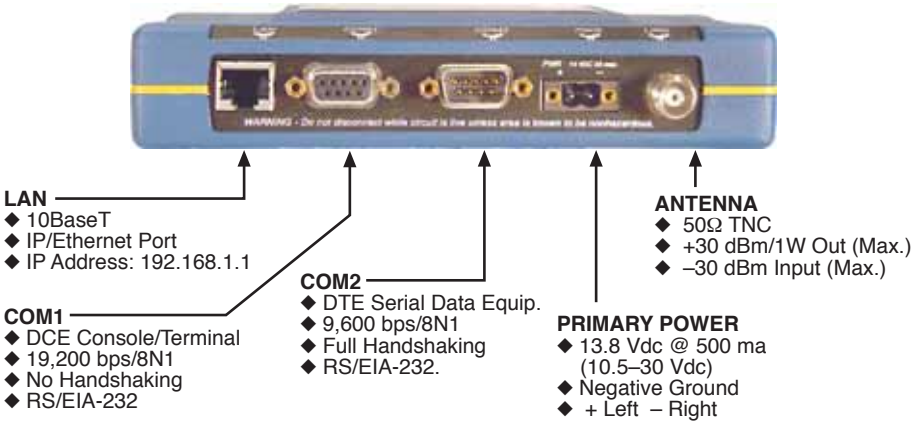


Figure 2-3. Interface Connectors, Functions & Defaults

2.7 STEP 6—CHECK FOR NORMAL OPERATION

Once the data equipment is connected, you are ready to check the transceiver for normal operation.

Observe the LEDs on the top cover for the proper indications. In a normally operating system, the following LED indications will be seen within 30 seconds of start-up:

- PWR—Lit continuously
- LINK—On, or blinking intermittently to indicate traffic flow
- LAN—On, or blinking intermittently to indicate traffic flow

Table 2-2 provides details on the LED functions.

Table 2-2. Transceiver LED Functions

LED Label	Activity	Indication
LAN	ON	LAN detected
	Blinking	Data TX/RX
	OFF	LAN not detected, or excessive traffic present
COM1 (MGT System)	Blinking	Data TX/RX
	OFF	No data activity
COM2	Blinking	Data TX/RX
	OFF	No data activity
PWR	ON	Primary power (DC) present
	Blinking	Unit in “Alarmed” state
	OFF	Primary power (DC) absent

Table 2-2. Transceiver LED Functions *(Continued)*

LED Label	Activity	Indication
LINK (Access Point)	ON	Default state
	Blinking	Data Tx/Rx
	OFF	Traffic exceeds the capacity of the radio network
LINK (Remote Gateway)	ON	Associated to AP
	Blinking	Data Tx/Rx
	OFF	Not associated with AP

If the radio network seems to be operating properly based on observation of the unit's LEDs, you can use the **PING** command to verify the link integrity with the Access Point or pointing your browser to another Remote unit's IP address in the same network.

3 EMBEDDED MANAGEMENT SYSTEM

Contents

3.1 MS INTRODUCTION 27
3.1.1 Differences in the User Interfaces 27
3.2 ACCESSING THE MENU SYSTEM 29
3.2.1 Methods of Control 30
3.2.2 PC Connection & Log In Procedures 30
3.2.3 Navigating the Menus 34
3.3 BASIC DEVICE INFORMATION 36
3.3.1 Starting Information Screen 36
3.3.2 Main Menu 37
3.3.3 Configuring Basic Device Parameters 38
3.4 CONFIGURING NETWORK PARAMETERS 40
3.4.1 Network Configuration Menu 40
3.4.2 IP Address Configuration Menu 42
3.4.3 Ethernet Port Configuration Menu 43
3.4.4 DHCP Server Configuration 44
3.4.5 SNMP Agent Configuration 46
3.5 RADIO CONFIGURATION 48
3.5.1 Radio Configuration Menu 48
3.5.2 Mobile Data Configuration 54
3.6 CONFIGURING THE SERIAL INTERFACES 56
3.6.1 Overview 56
3.6.2 Serial Data Port Configuration Menu 59
3.6.3 Configuring for UDP Mode 60
3.6.4 Configuring for TCP Mode 64
3.6.5 Configuring for PPP Mode 66
3.6.6 IP-to-Serial Application Example 67
3.6.7 Point-to-Point Serial-to-Serial Application Example 68
3.6.8 Point-to-Multipoint Serial-to-Serial Application Example 69
3.6.9 Mixed Modes 71
3.7 SECURITY CONFIGURATION 73

3.7.1 Approved Remotes/Access Points List Menu 75

3.8 PERFORMANCE VERIFICATION 76

3.8.1 Performance Information Menu 76
3.8.2 Network Performance Notes 87

3.9 MAINTENANCE..... 91

3.9.1 Reprogramming Menu 92
3.9.2 Configuration Scripts Menu 97
3.9.3 Authorization Keys Menu 105
3.9.4 Auto-Upgrade/Remote-Reboot Menu 106
3.9.5 Radio Test Menu 107
3.9.6 Ping Utility Menu 108
3.9.7 Reset to Factory Defaults 108
3.9.8 Resetting the Password 108

3.1 MS INTRODUCTION

The transceiver's embedded management system is accessible through various data interfaces. These include the COM1 (serial) port, LAN (Ethernet) port, and via SNMP. Essentially the same capabilities are available through any of these paths.

For SNMP management, the transceiver is compatible with MDS *NETview MS*™ software. Refer to MDS publication 05-2973A01 for more information on this tool. For support of other SNMP software, a set of MIB files is available for download from the MDS Web site at **www.microwavedata.com**. A brief summary of SNMP commands can be found at *SNMP Agent Configuration* section on Page 46 of this manual.

The transceiver's Management System and its functions are divided into five functional groups as listed below.

- Section 3.3, *BASIC DEVICE INFORMATION* (beginning on Page 36)
- Section 3.4, *CONFIGURING NETWORK PARAMETERS* (beginning on Page 40)
- Section 3.5, *RADIO CONFIGURATION* (beginning on Page 48)
- Section 3.6, *CONFIGURING THE SERIAL INTERFACES* (beginning on Page 56)
- Section 3.7, *SECURITY CONFIGURATION* (beginning on Page 73)
- Section 3.8, *PERFORMANCE VERIFICATION* (beginning on Page 76)
- Section 3.9, *MAINTENANCE* (beginning on Page 91)

Each of these sections has a focus that is reflected in its heading. The section you are now reading provides information on connecting to the Management System, how to navigate through it, how it is structured, and how to perform top-level configuration tasks. Figure 3-1 on the following page shows a top-level view of the Management System (MS).

3.1.1 Differences in the User Interfaces

There are slight differences in navigation, but for the most part, the content is the same among different user interfaces. You will find a few differences in capabilities as the communications tool is driven by limitations of the access channel. Below are examples of the Starting Information Screen seen through a terminal and a Web-browser, respectively.

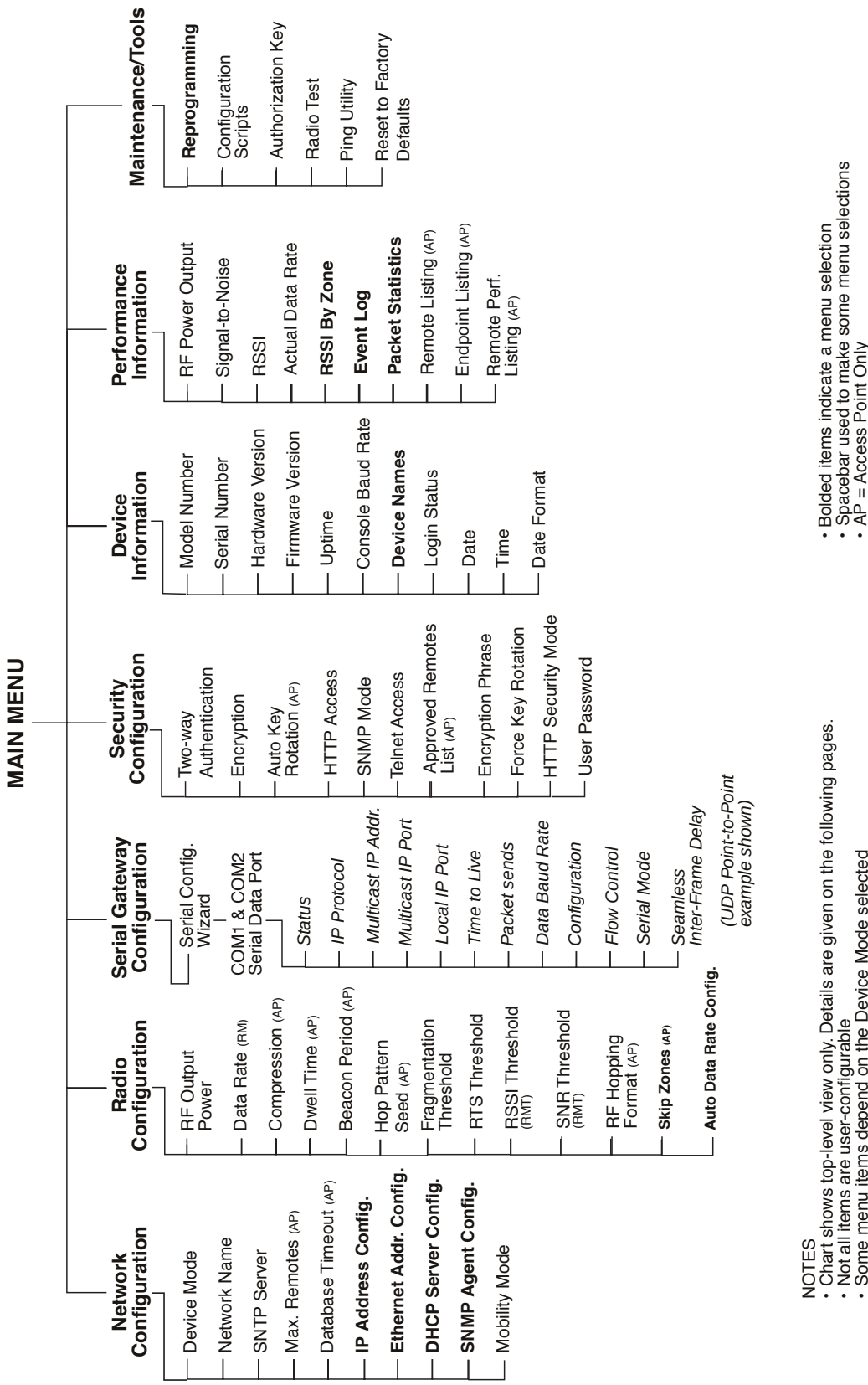


Figure 3-1. Embedded Management System—Top-level Flowchart

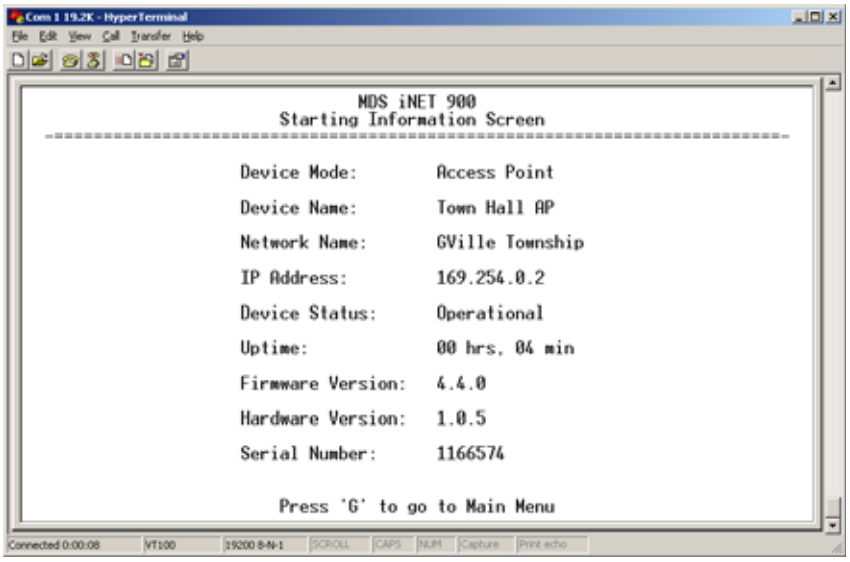


Figure 3-2. View of MS with a text-based program—(Terminal Emulator shown—Telnet has similar menu structure)

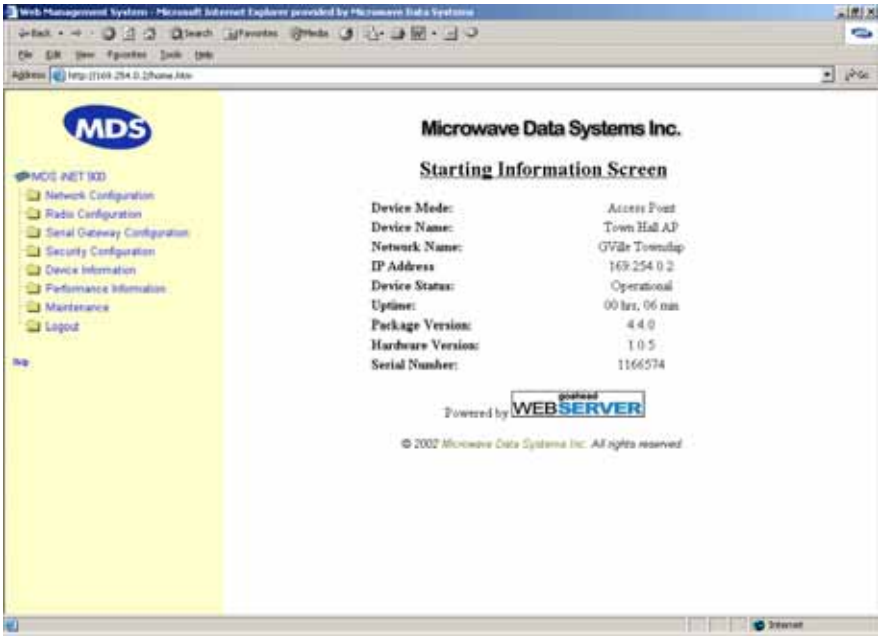


Figure 3-3. View of the MS with a Browser

3.2 ACCESSING THE MENU SYSTEM

The radio has no external controls. All configuration, diagnostics and control is performed electronically using a connected PC. This section explains how to connect a PC, log into the unit, and gain access to the built-in menu screens.

3.2.1 Methods of Control

The unit's configuration menus may be accessed in one of several ways:

- **Local Console**—*This is the primary method used for the examples in this manual*. Connect a PC directly to the COM 1 port using a serial communications cable and launch a terminal communications program such as HyperTerminal. This method provides text-based access to the unit's menu screens. Console control is a hardware-based technique, and is intended for local use only.
- **Telnet***—Connect a PC to the unit's LAN port, either directly or via a network, and launch a Telnet session. This method provides text-based access to the unit's menu screens in a manner similar to a Local Console session. Telnet sessions may be run locally or remotely through an IP connection.
- **Web Browser***—Connect a PC to the unit's LAN port, either directly or via a network, and launch a web browser session (*i.e.*, Internet Explorer, Netscape, etc.) This method provides a graphical representation of each screen, just as you would see when viewing an Internet website. The appearance of menu screens differs slightly from other methods of control, but the content and organization of screen items is similar. Web browser sessions may be run locally or remotely via the Internet.

* Telnet and Web Browser sessions require the use of a *straight-through* or *crossover* Ethernet cable, depending on the whether the PC-to-radio connection is made directly, or through a network. For direct connection, a **crossover** cable is required; For connection via a network, a **straight-through** type is needed.

Cable type can be identified as follows: Hold the two cable ends side-by-side and in the same plug orientation (*i.e.*, both locking tabs up or down). Now look at the individual wire colors on each plug. If the wires on both plugs are ordered in the same sequence from left to right, the cable is a straight-through type. If they are not in the same order, it *may* be a crossover cable, or it may be wired for some other application. Refer to *DATA INTERFACE CONNECTORS* on Page 143 for detailed pinout information.

3.2.2 PC Connection & Log In Procedures

The following steps describe how to access the radio's menu system. These steps require a PC to be connected to the unit's COM 1 or LAN port as shown in Figure 3-4.

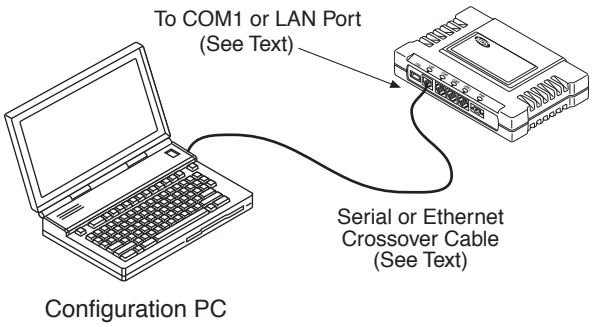


Figure 3-4. PC Configuration Setup

Starting a Local Console Session (Recommended for first-time Users)

1. Connect a serial communications cable between the PC and the unit's COM 1 port. If necessary, a cable may be constructed for this purpose as shown in Figure 3-5.

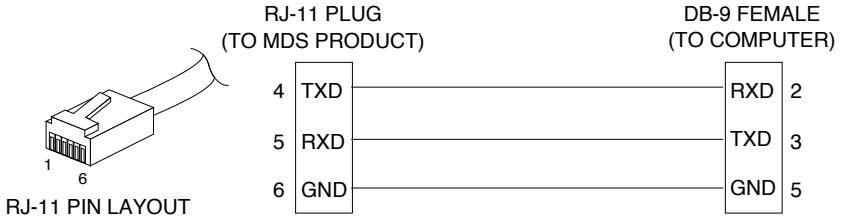


Figure 3-5. Serial Communications Cable (RJ-11 to DB-9)
(Maximum Recommended Cable Length 50 Feet/15 meters)

2. Launch a terminal emulation program such as HyperTerminal and configure the program with the following settings:
   - 19,200 bps data rate
   - 8 data bits, no parity
   - One stop bit, and no flow-control
   - Use ANSI or VT100 emulation.

TIP: The HyperTerminal communications program can be accessed on most PCs by selecting this menu sequence: **Start>>Programs>>Accessories>>Communications>>HyperTerminal.**

NOTE: The *exact* parameters given above must be used for console terminal communication. Improper settings are a common cause of difficulty.

NOTE: If the unit is powered-up or rebooted while connected to a terminal, you will see a series of pages of text information relating to the booting of the unit's microcomputer. Wait for the log-in screen before proceeding.

3. Press the ENTER key to receive the **login:** prompt.

4. Enter the username (default username is **admin**). Press ENTER.

5. Enter your password (default password is **admin**). (For security, your password keystrokes do not appear on the screen.) Press ENTER.

NOTE: Passwords are case sensitive. Do not use punctuation mark characters. You may use up to eight alpha-numeric characters.

The unit responds with the Starting Information Screen (Figure 3-6). From here, you can review basic information about the unit or press **G** to proceed to the Main Menu.

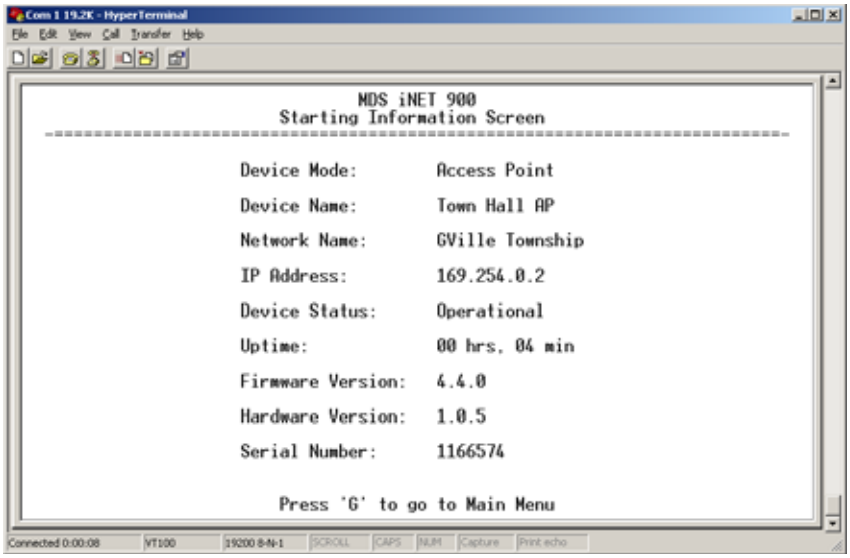


Figure 3-6. Starting Information Screen—Local Console Session
(Telnet has similar menu structure)

Starting a Telnet Session

NOTE: This method requires that you know the IP address of the unit beforehand. If you do not know the address, use the Local Console method (above) and access the *Starting Information Screen*. The address is displayed on this screen.

1. Connect a PC to the unit's LAN port, either directly or via a network. If connecting directly, use an Ethernet *crossover* cable; if connecting via a network, use a *straight-through* cable. The LAN LED lights to indicate an active connection.

NOTE: When using a Local Area Network (LAN) to access the unit, it may be necessary to change your computer's IP access to the LAN in order to be compatible with the entraNET (compatible subnets). You can identify or verify the unit's IP address by using a Local Console session to communicate with the entraNET through its COM 1 Port and viewing the *Starting Information Screen*.

2. Start the Telnet program on your computer targeting the IP address of the unit to which you are connected. and press ENTER.

TIP: A Telnet session can be started on most PCs by selecting: **Start>>Programs>>Accessories>>Command Prompt**. At the command prompt window, type the word **telnet**, followed by the unit's IP address (*e.g.*, **telnet 10.1.1.168**). Press ENTER to receive the Telnet log in screen.

NOTE: Never connect multiple units to a network with the same IP address. Address conflicts will result in improper operation.

---

3. Enter your username (default username is **admin**). Press ENTER.

   Next, the **Password:** prompt appears. Enter your password (default password is **admin**). (For security, your password keystrokes will not appear on the screen.) Press ENTER.

   The unit responds with a Starting Information Screen (see Figure 3-6). From here, you can review basic information about the unit or press **G** to proceed to the Main Menu.

NOTE: Passwords are case sensitive. Do not use punctuation mark characters. You may use up to eight alpha-numeric characters.

Starting a Web Browser Session

NOTE: Web access requires that you know the IP address of the unit you are connecting to. If you do not know the address, start a Local Console session (see *Starting a Local Console Session (Recommended for first-time Users)* on Page 31) and access the *Starting Information Screen*. The IP address is displayed on this screen.

---

1. Connect a PC to the unit's LAN port, either directly or via a network. If connecting directly, use an Ethernet *crossover* cable; if connecting via a network, use a *straight-through* cable. The LAN LED lights to indicate an active connection.

2. Launch a Web-browser session on your computer (*i.e.*, Internet Explorer, Netscape Navigator, etc.).

3. Type in the unit's IP address and press ENTER.

4. A log-in screen is displayed (Figure 3-7) where you enter a user name and password to access the unit's menu system. Note that the default entries are made in *lower case*. (Default User Name: **admin**; Default Password: **admin**)

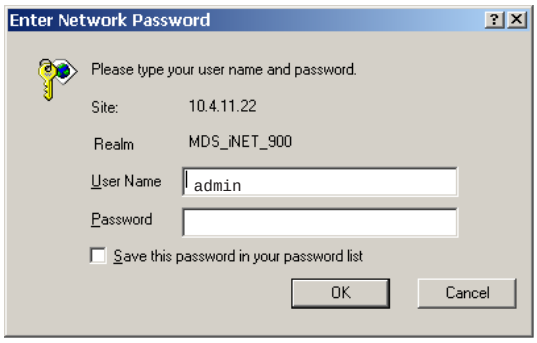


Figure 3-7. Log-in Screen when using a Web Browser

NOTE: Passwords are case sensitive. Do not use punctuation mark characters. You may use up to eight alpha-numeric characters.

5. Click **OK**. The unit responds with a startup menu screen similar to that shown in Figure 3-8. From here, you can review basic information about the unit or click on one of the menu items at the left side of the screen.

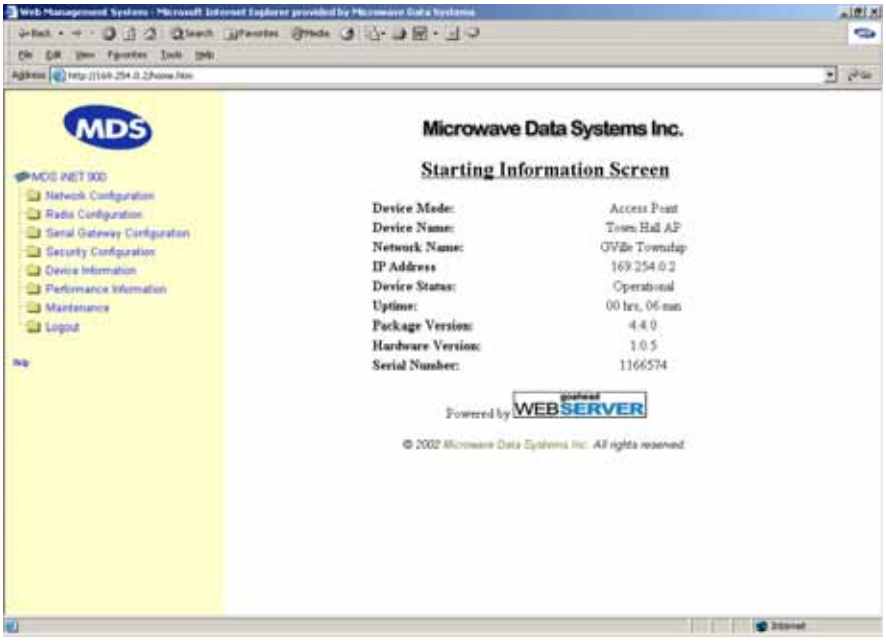


Figure 3-8. Starting Information Screen—Web Browser Example

3.2.3 Navigating the Menus

Via Terminal or Telnet Sessions—*Recommended for first-time users*

Local Console and Telnet sessions use multi-layered text menu systems that are nearly identical. To move further down a menu tree, you type the letter assigned to an item of interest. This takes you to an associated screen where settings may be viewed, or changed. In most cases,

pressing the ESCAPE key moves the screen back one level in the menu tree.

In general, the top portion of menu screens show *read-only* information (with no user selection letter). The bottom portion of the screen contains parameters that can be selected for further information, alteration of values, or to navigate to other submenus.

When you arrive at a screen with user-controllable parameter fields, you select the menu item by pressing an associated letter on the keyboard. If there is a user definable value, the field will clear to the right of the menu item and you can type in the value you wish to use. Follow this action by pressing the ENTER key to save the changes. If you make a mistake or change your mind before pressing the ENTER key, simply press ESCAPE to restore the previous value.

In some cases, when you type a letter to select a parameter, you will see a prompt at the bottom of the screen that says **Choose an Option**. In these screens, press the keyboard's SPACEBAR to step through the available selections. When the desired option appears, press the ENTER key to choose that selection. In some cases, several parameters may be changed and then saved by a single keystroke. The ESCAPE key can be used to cancel the action and restore the previous values.

Logging Out Via Terminal Emulator or Telnet

From the Main Menu screen, press **Q** to quit and terminate the session.

Navigating via Web Browser

Navigating with a Web browser is straightforward with a framed "homepage." The primary navigation menu is permanently located on the left-hand side of this page. Simply click on a desired menu item to bring it to the forefront.

NOTE: To maintain security, it is best to log-out of the menu system entirely when you are done working with it. If you do not log out, the session automatically ends after 10 minutes of inactivity.

Logging Out Via Web Browser

Click on **Logout** in the left-hand frame of the browser window. The right-hand frame will change to a logout page. Follow the remaining instructions on this screen.

NOTE: In the menu descriptions that follow, parameter options/range, and any default values are displayed at the end of the text between square brackets. Note that the default setting is always shown after a semicolon: [**available settings or range; default setting**]

3.3 BASIC DEVICE INFORMATION

This section contains detailed menu screens and settings that you can use to specify the behavior of the unit.

3.3.1 Starting Information Screen

Once you have logged into the Management System, you will be presented with a screen that provides an overview of the transceiver and its current operating condition. It provides an array of vital information and operating conditions.

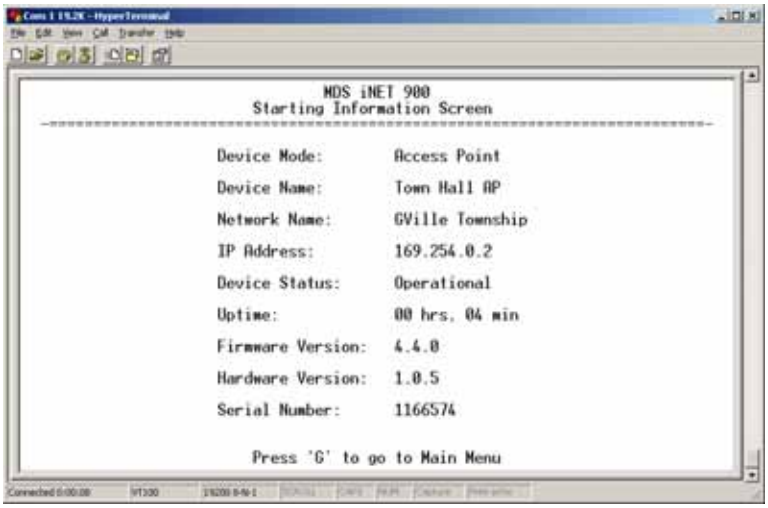


Figure 3-9. Starting Information Screen

- **Device Mode**—Current operating mode of the unit as it relates to the radio network.
- **Device Name**—This is a user-defined parameter that will appear in the heading of all pages.
  (To change it, see *Network Configuration Menu* on Page 40.)
- **Network Name**—The name of the radio network in which the unit is associated.
- **IP Address**—Unit's IP address [**192.168.1.1**]
- **Device Status**—Condition of the unit's association with an Access Point.

  At the Access Point:
  - *Alarmed*—A alarm event has been logged and not cleared.
  - *Operational*—Unit operating normally.

  At a Remote:
  - *Scanning*—The unit is looking for an Access Point beacon signal.
  - *Exp(ecting) Sync(hronization)*—The unit has found a valid beacon signal for its network.

- *Hop Sync*—The unit has changed its frequency hopping pattern to match that of the Access Point.
- *Associated* —This unit has successfully synchronized and associated with an Access Point.
- *Alarmed*—The unit is has detected one or more alarms that have not been cleared.

NOTE: If an alarm is present when this screen is displayed, an "A)" appears to the left of the **Device Status** field. Pressing the "A" key on your keyboard takes you directly to the "Current Alarms" screen.

- **Uptime**—Elapsed time since the transceiver was powered-up.
- **Firmware Version**—Version of firmware that is currently active in the unit.
- **Hardware Version**— Hardware version of the transceiver's printed circuit board.
- **Serial Number**—Make a record of this number. It must be provided to purchase Authorization Keys to upgrade unit capabilities. (See *"Authorization Keys Menu"* on Page 105.)

3.3.2 Main Menu

The next screen, the Main Menu, is the entryway to all user-controllable features. The transceiver's **Device Name** appears at the top of this and all other screens as a reminder of the unit that is currently being controlled

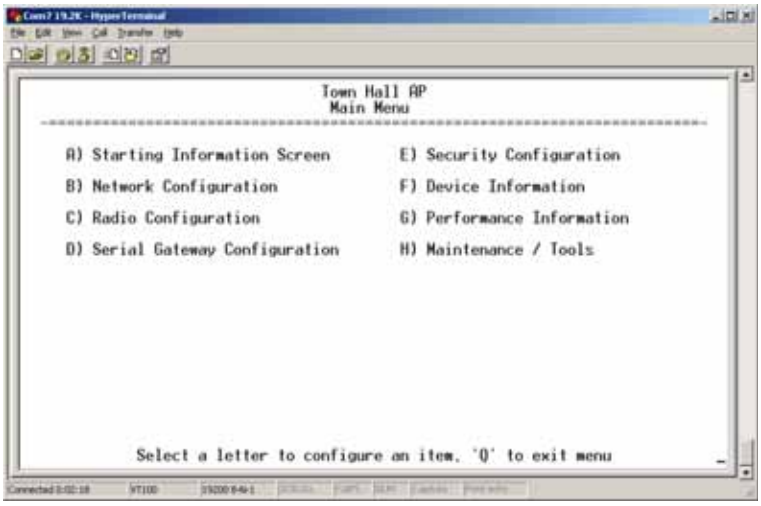


Figure 3-10. Main Menu

- **Starting Information Screen**—Select this item to return to the start-up screen. (See *"Starting Information Screen"* on Page 36)
- **Network Configuration**—Tools to configure the data network layer of the transceiver. (See *"Network Configuration Menu"* on Page 40)

- **Radio Configuration**—Tools to configure the wireless (radio) layer of the transceiver. (See *"Radio Configuration Menu"* on Page 48)
- **Serial Gateway Configuration**—Tools to configure the two serial ports. (See *"Serial Data Port Configuration Menu"* on Page 59)
- **Security Configuration**—Tools to configure the security services available with the transceiver's environment. (See *"SECURITY CONFIGURATION"* on Page 73)
- **Device Information**—Top level user-specific and definable parameters, such as unit password. (See *"Device Information"* on Page 38)
- **Performance Information**—Tools to measure the radio and data layer's performance of the radio network. (See *"Performance Information Menu"* on Page 76)
- **Maintenance/Tools**—Tools to use configuration files, change firmware and use Authorization Keys to change major unit capabilities. (See *"Authorization Key—Alter the unit's overall capabilities by enabling the built-in resources. (See "Authorization Keys Menu" on Page 105)"* on Page 91)

3.3.3 Configuring Basic Device Parameters

Device Information

Below is the menu/screen that displays basic administrative data on the unit to which you are connected. It also provides access to some user-specific parameters such as device names.

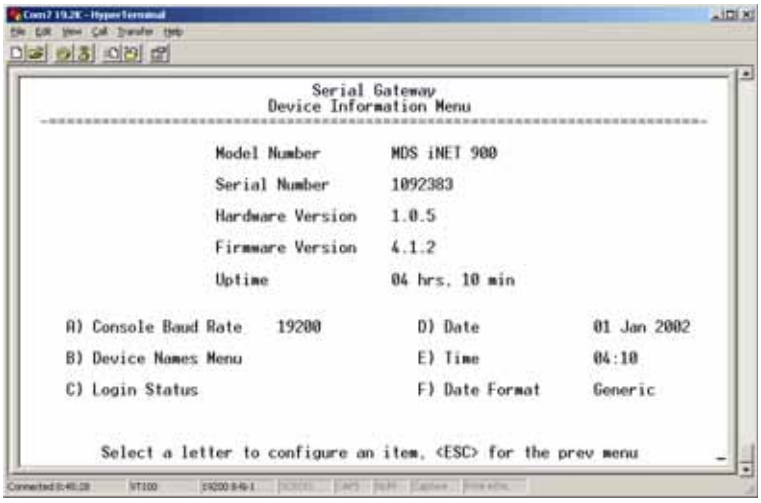

Serial Gateway
Device Information Menu
Model Number MDS iNET 900
Serial Number 1092383
Hardware Version 1.0.5
Firmware Version 4.1.2
Uptime 04 hrs, 10 min
A) Console Baud Rate 19200
B) Device Names Menu
C) Login Status
D) Date 01 Jan 2002
E) Time 04:10
F) Date Format Generic
Select a letter to configure an item, <ESC> for the prev menu

Figure 3-11. Device Information Menu

- **Model Number** *(Display only)*
- **Serial Number** *(Display only)*
- **Hardware Version** *(Display only)*
- **Firmware Version** *(Display only)*—Current firmware installed and being used by the transceiver.

- **Uptime** *(Display only)*—Elapsed time since powering up.
- **Device Names Menu**—Fields used at user's discretion for general administrative purposes. The Device Name field is used by the transceiver as the "Realm" name for network security and in the MS screen headings. (See Figure 3-12 on Page 39)
- **Date**—Current date being used for the transceiver logs. User-setable. (Value lost with power failure if SNTP (Simple Network Time Protocol) server not accessible.)
- **Time**—Current time of day. User-setable.
  Setting: HH:MM:SS
  (Value lost with power failure if SNTP server not accessible.)
- **Date Format**—Select presentation format:
  - Generic = dd Mmm yyyy
  - European = dd-mm-yyyy
  - US = mm-dd-yyyy

Device Names Menu

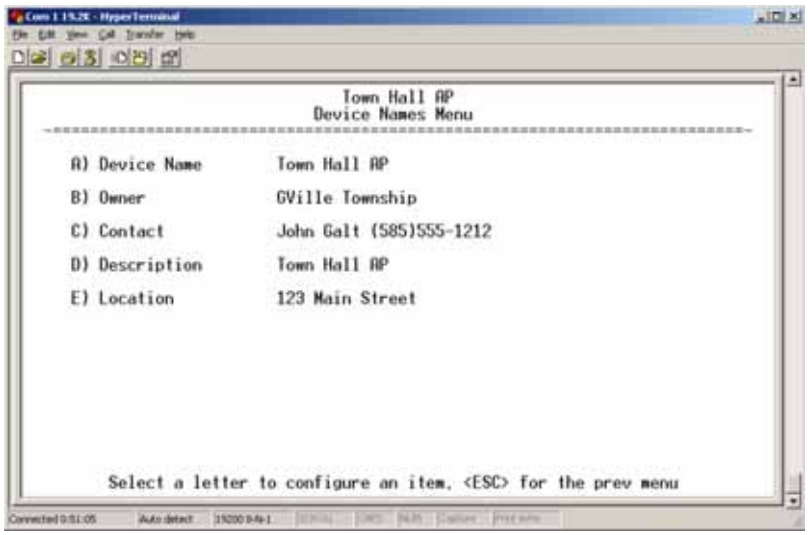

Town Hall AP
Device Names Menu
A) Device Name Town Hall AP
B) Owner GVille Township
C) Contact John Galt (585)555-1212
D) Description Town Hall AP
E) Location 123 Main Street
Select a letter to configure an item, <ESC> for the prev menu

Figure 3-12. Device Names Menu

- **Device Name**—Device Name, used by the transceiver as the "Realm" name for network login (web browser only) and menu headings.
- **Owner**—User defined; appears on this screen only.
- **Contact**—User defined; appears on this screen only.
- **Description**—User defined; appears on this screen only.
- **Location**—User defined; appears on this screen only.

3.4 CONFIGURING NETWORK PARAMETERS

3.4.1 Network Configuration Menu

The *Network Configuration Menu* is the home of three parameters that should be reviewed and changed as necessary before placing a transceiver in service—Device Mode, IP Address and Network Name. Screens for both the Access Point and Remote units are shown below.

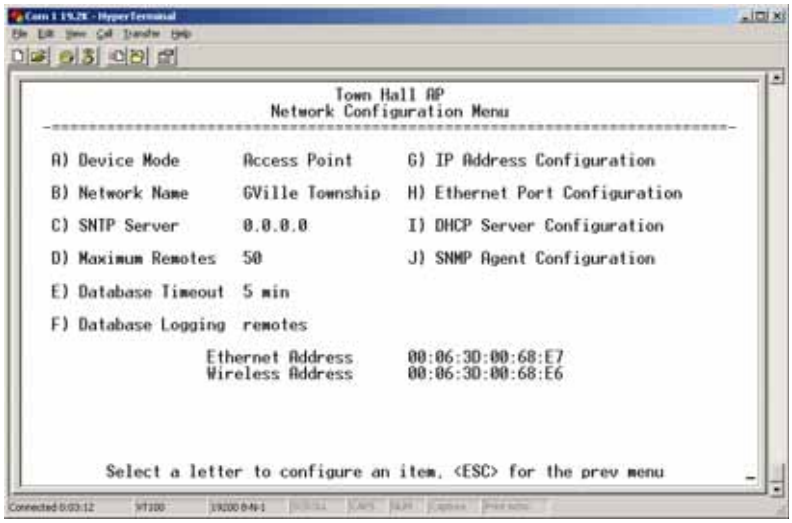

Town Hall AP
Network Configuration Menu
A) Device Mode Access Point
B) Network Name GVille Township
C) SNTP Server 0.0.0.0
D) Maximum Remotes 50
E) Database Timeout 5 min
F) Database Logging remotes
G) IP Address Configuration
H) Ethernet Port Configuration
I) DHCP Server Configuration
J) SNMP Agent Configuration
Ethernet Address 00:06:3D:00:68:E7
Wireless Address 00:06:3D:00:68:E6
Select a letter to configure an item, <ESC> for the prev menu

Figure 3-13. Network Configuration Menu
From Access Point

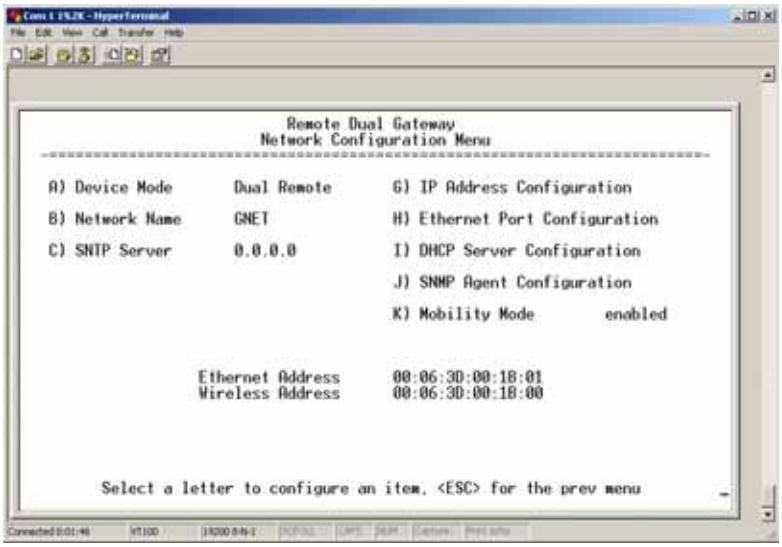

Remote Dual Gateway
Network Configuration Menu
A) Device Mode Dual Remote
B) Network Name GNET
C) SNTP Server 0.0.0.0
G) IP Address Configuration
H) Ethernet Port Configuration
I) DHCP Server Configuration
J) SNMP Agent Configuration
K) Mobility Mode enabled
Ethernet Address 00:06:3D:00:1B:01
Wireless Address 00:06:3D:00:1B:00
Select a letter to configure an item, <ESC> for the prev menu

Figure 3-14. Network Configuration Menu
From Remote Unit

- **Device Mode** *(User Review Recommended)*—Either Access Point or a variation of a Remote. [**Remote**]
- **Network Name** *(User Review Required)*—Name of the radio network of which this unit will be a part. Essential for association of Remotes to the Access Point in the network. [**Not Programmed**]

TIP: For enhanced security, consider using misspelled words, a combination of letters and numbers, and a combination of upper and lower case letters. Also, the Network Name should be at least nine characters long. This helps protect against sophisticated hackers who may use a database of common words (for example, dictionary attacks) to determine the Network Name.

- **SNTP Server**—Address of SNTP server (RFC 2030) from which the transceiver will automatically get the time-of-day startup time. Without an SNTP server, the date and time must be manually set. An AP will try to get the time and date from the SNTP server only if an IP address is configured. It will continue to retry every minute until it succeeds.

  A remote will get the time and date from the SNTP server, if an IP address is configured. Otherwise it gets it from the AP at authentication time. The transceivers use UTC (Universal Time Constant) with a configurable time offset. [**0.0.0.0**]
- **IP Address Configuration** Presents a menu for configuring the local static IP address of the transceiver. Detailed explanations are provided in the section titled *IP Address Configuration Menu* on Page 42
- **Ethernet Port Configuration**—Presents a menu for defining the status of the Ethernet port (enabled or disabled), the Ethernet rate limit, link hardware watch (enabled/disabled), and the Ethernet link poll address. Detailed explanations of this menu are contained in *Ethernet Port Configuration Menu* on Page 43
- **DHCP Server Config(uration)**—Menu for configuration of DHCP services by the Access Point unit. DHCP provides “on-the-fly” IP address assignments to other LAN devices, including MDS *i*NET 900 units. [**Disabled**]
- **SNMP Config Menu**—SNMP configuration parameters.
- **Mobility Mode**—Here, you determine whether the transceiver is enabled or disabled for mobility operation. *Note that this selection may appear on both Access Point and Remote menus, but it only takes effect when set on Remotes.* Additional settings and information for mobility operation are contained in *Mobile Data Configuration* on Page 54. [**enabled, disabled; disabled**].
- **Maximum Remotes** *(AP Only)*—Number of Remotes permitted to be associated with (served by) this Access Point. [**50**]

- **Database Timeout** *(AP Only)*—This sets the database "age time" (*Remote Listing Menu (Access Points Only)* on Page 84) to determine when a remote is declared as unavailable. The timer may be set from 0 to 255 minutes and resets each time a message is received from a remote. [**0–255 minutes; 5 minutes**]
- **Database Logging** *(AP Only)*—Determines which types of devices will be reported as "added" or "deleted" from the AP's database (See Section 3.8.1, *Performance Information Menu* (beginning on Page 76). In the case of deletions, this information is triggered by a timer expiration as described in the item above. Available selections are: **Remote**, **All** (endpoints and remotes), or **Disabled**.
- **Ethernet Address** *(Display Only)*—Hardware address of this unit's Ethernet interface.
- **Wireless Address** *(Display Only)*—Hardware address of the unit's wireless interface.

3.4.2 IP Address Configuration Menu

The radios use a local IP address to support remote management and serial device services. The IP address of a radio can be set as a *static IP address* or as a *dynamic IP address*. When static IP addressing is used, the user must manually configure the IP address and other parameters. When dynamic addressing is used, the radio uses a DHCP Client process to obtain an IP address from a DHCP Server, along with other parameters such as a *net mask* and a *default gateway*.

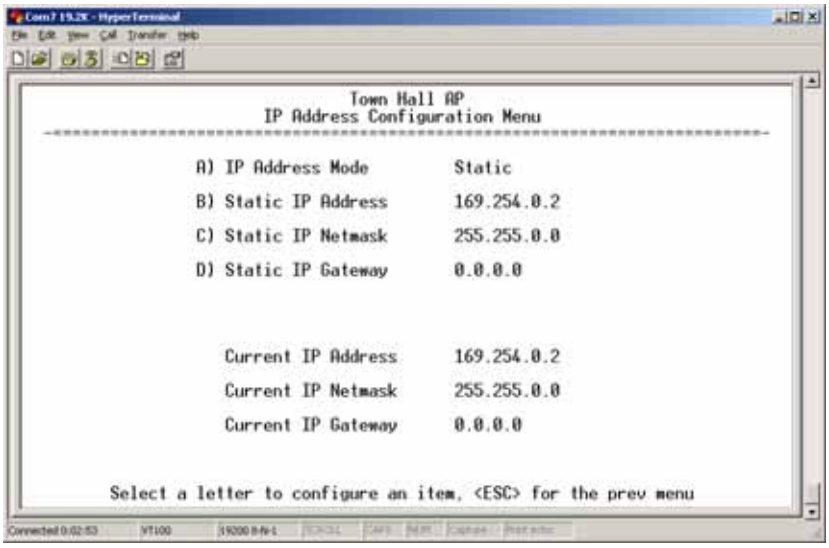

Town Hall AP
IP Address Configuration Menu
A) IP Address Mode Static
B) Static IP Address 169.254.0.2
C) Static IP Netmask 255.255.0.0
D) Static IP Gateway 0.0.0.0
Current IP Address 169.254.0.2
Current IP Netmask 255.255.0.0
Current IP Gateway 0.0.0.0
Select a letter to configure an item, <ESC> for the prev menu

Figure 3-15. IP Address Configuration Menu

CAUTION: Changes to any of the following parameters while communicating over the network (LAN or over-the-air) may cause a loss of communication with the unit being configured. Communication will need to be re-established using the new IP address.

- **IP Address Mode**—Defines the source of the IP address of this device. [**Static, Dynamic; Static**]
- **Dynamic Mode**—Enabling this option forces the transceiver (AP or Remote) to obtain an IP address from any DHCP server available on the LAN. Dynamic Mode is also known as *DHCP Client* mode. [**Disabled**]
- **Static IP Address** *(User Review Recommended)*—Essential for connectivity to the transceiver's MS via the LAN port and to send Ethernet data over the network. Enter any valid IP address that will be unique within the network. [**192.168.1.1**]
  This field is unnecessary if DHCP is enabled. [**255.255.0.0**]

  Static IP Netmask—The IPv4 local subnet mask. This field is unnecessary if DHCP is enabled. [**255.255.0.0**]
- **Static IP Gateway**—The IPv4 address of the network gateway device, typically a router. This field is unnecessary if DHCP is enabled. [**0.0.0.0**]

  The lower three lines of the screen show the actual addressing at the transceiver whether it was obtained from static configuration or from a DHCP server.

NOTE: Any change made to the above parameters results in the **Commit Changes** option appearing on screen. This allows all IP settings to be changed at the same time.

3.4.3 Ethernet Port Configuration Menu

The transceiver allows for special control of the Ethernet interface, to allow traffic awareness and availability of the backhaul network for redundancy purposes.

NOTE: The *i*NET 900 network port supports 10BaseT connections, but does not support 100BaseT connections. This should not present a problem because most hubs/switches auto-switch between 10BaseT and 100BaseT connections. Confirm that your hub/switch is capable of auto-switching data rates.

To prevent Ethernet traffic from degrading *i*NET 900 performance, place the *i*NET in a segment, or behind routers.

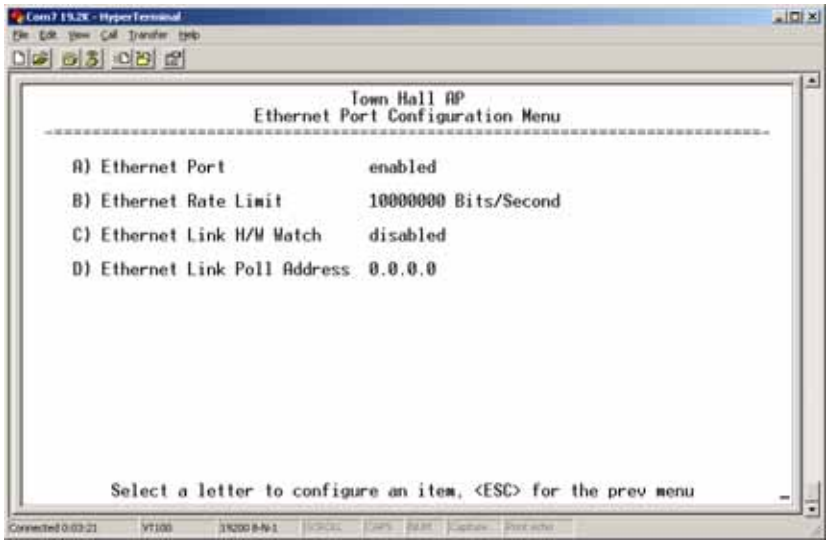

Town Hall AP
Ethernet Port Configuration Menu
A) Ethernet Port enabled
B) Ethernet Rate Limit 10000000 Bits/Second
C) Ethernet Link H/W Watch disabled
D) Ethernet Link Poll Address 0.0.0.0
Select a letter to configure an item, <ESC> for the prev menu

Figure 3-16. Ethernet Port Configuration Menu

- **Ethernet port enabled/disabled**—Allows remote disabling of Ethernet traffic for security purposes. [**Enabled, Disabled; Enabled**]
- **Ethernet Rate Limit**—The transceiver will send alarms (SNMP traps) when the rate reaches 50%, 75%, and 100% to help identify potential problems with traffic.
- **Ethernet Link (H/W) Watch** *(AP Only)*—Detects the lack of an Ethernet connection to the LAN port at the electrical level (link integrity). The current AP will broadcast a beacon signal indicating its "NOT AVAILABLE" status so Remotes that hear it do not try to associate to it. Once the Ethernet connection is restored, this beacon signal changes to "AVAILABLE" and Remotes are allowed to join in. [**Disabled**]
- **Ethernet Link Poll Address** *(AP Only)*—When an IP address is provided, the Access Point pings the remote IP device every 2 minutes to test the integrity of the backhaul link. If this link is not available, the AP will advertise its "NOT AVAILABLE" status in the beacon signal so Remotes do not try to associate to it. Once the IP address is reachable, this beacon signal changes to "AVAILABLE" and Remotes are allowed to join in. 0.0.0.0 disables this function. Any other valid IP address enables it. [**0.0.0.0**]

3.4.4 DHCP Server Configuration

A transceiver can provide automatic IP address assignments to other IP devices in the network by providing DHCP (Dynamic Host Configuration Protocol) services. This service eliminates setting individual device IP address on Remotes in the network, but it still requires thoughtful planning of the IP address range. One drawback to network-wide auto-

matic IP address assignments is that SNMP services may become inaccessible as they are dependent on fixed IP addresses.

The network can be comprised of radios with the DHCP-provided IP address enabled or with DHCP services disabled. In this way, you can accommodate locations for which a fixed IP address if desired.

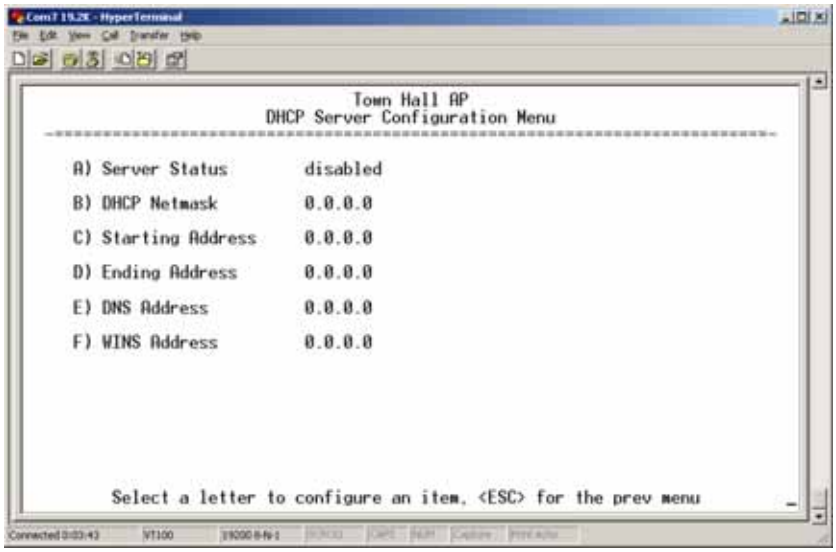

Town Hall AP
DHCP Server Configuration Menu
A) Server Status disabled
B) DHCP Netmask 0.0.0.0
C) Starting Address 0.0.0.0
D) Ending Address 0.0.0.0
E) DNS Address 0.0.0.0
F) WINS Address 0.0.0.0
Select a letter to configure an item, <ESC> for the prev menu

Figure 3-17. DHCP Server Configuration Menu

NOTE: There should be only one DHCP server active in a network (MDS *i*NET 900 or other DHCP server). If more than one DHCP server exists, network devices may randomly get their IP address from different servers every time they request one.

- **Server Status**—Enable/Disable responding to DHCP requests to assign an IP address. [**Disabled/Enabled; Disabled**]
- **DHCP Netmask**—IP netmask to be assigned along with the IP address in response to a DHCP request. [**0.0.0.0**]
- **Starting Address**—Lowest IP address of the range of addresses to be provided by this device. [**0.0.0.0**]
- **Ending Address**—Highest IP address in the range of addresses to be provided by this device. A maximum of 256 addresses is allowed in this range. [**0.0.0.0**]
- **DNS Address**—Domain Name Server address to be provided by this service.
- **WINS Address**—Windows Internet Naming Service server address to be provided by this service.
- **Restart DHCP Server**—Selecting this option forces the transceiver to start servicing DHCP requests using the Starting Address. Payload data will not be interrupted but may experience some delays as new addresses are distributed.

3.4.5 SNMP Agent Configuration

The transceiver contains over 100 custom SNMP-manageable objects as well as the IETF standard RFC1213 for protocol statistics, also known as MIB II. Off-the-shelf SNMP managers such as Castle Rock Computing *SNMPc*™ and Hewlett Packard HP *OpenView*™ may also be used to access the transceiver's SNMP Agent's MIB. The transceiver's SNMP agent supports SNMPv3.

The objects are broken up into nine MIB files for use with your SNMP manager. There are textual conventions, common files and specific files. This allows the flexibility to change areas of the MIB and not affect other existing installations or customers.

- **msdreg.mib**—MDS sub-tree registrations
- **mds_comm.mib**—MDS Common MIB definitions for objects and events which are common to the entire product family
- **inet_reg.mib**—MDS sub-tree registrations
- **inettrv1.mib**—SNMPv1 enterprise-specific traps
- **inettrv2.mib**—SNMPv2 enterprise-specific traps
- **inet_comm.mib**— MIB definitions for objects and events which are common to the entire *i*NET Series
- **inet_ap.mib**—MIB definitions for objects and events for an Access Point transceiver
- **inet_sta.mib**—Definitions for objects and events for a Remote radio
- **inet_sec.mib**—For security management of the radio system. SNMPv3 allows read/write operation. SNMPv1/2 allows only for read-only access.

NOTE: SNMP management requires that the proper IP address, network and gateway addresses are configured in each transceiver of the associated network.

In addition, some management systems may require the MIB files to be compiled in the order shown above.

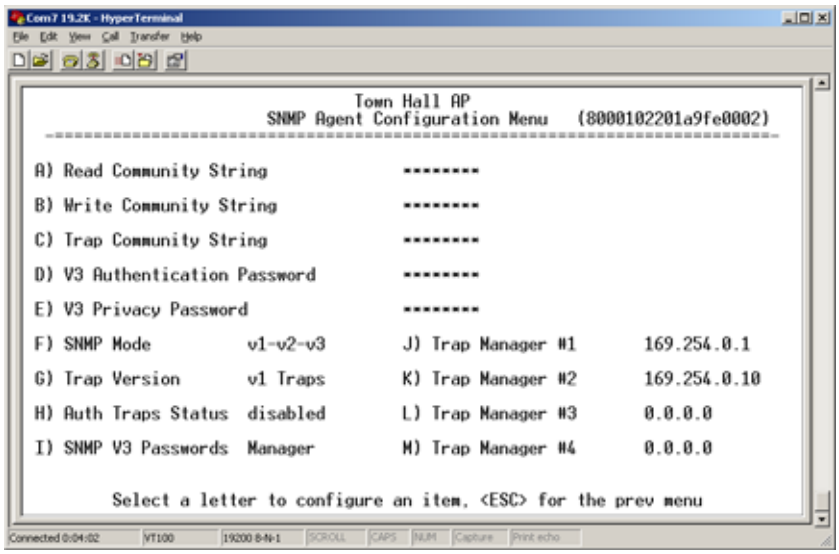

Com7 19.2K - HyperTerminal
File Edit View Call Transfer Help
Town Hall AP
SNMP Agent Configuration Menu (8000102201a9fe0002)
A) Read Community String ********
B) Write Community String ********
C) Trap Community String ********
D) V3 Authentication Password ********
E) V3 Privacy Password ********
F) SNMP Mode v1-v2-v3
G) Trap Version v1 Traps
H) Auth Traps Status disabled
I) SNMP V3 Passwords Manager
J) Trap Manager #1 169.254.0.1
K) Trap Manager #2 169.254.0.10
L) Trap Manager #3 0.0.0.0
M) Trap Manager #4 0.0.0.0
Select a letter to configure an item, <ESC> for the prev menu
Connected 0:04:02
VT100
19200 8-N-1
SCROLL
CAPS
NUM
Capture
Print echo

Figure 3-18. SNMP Server Configuration Menu
From Access Point

This menu provides configuration and control of vital SNMP functions.

- **Read Community String**—SNMP community name with SNMPv1/SNMPv2c read access. This string can be up to 30 alpha-numeric characters.
- **Write Community String**—SNMP community name with SNMPv1/SNMPv2c write access. This string can be up to 30 alpha-numeric characters.
- **Trap Community String**—SNMP community name with SNMPv1/SNMPv2c trap access. This string can be up to 30 alpha-numeric characters.
- **V3 Authentication Password**—Authentication password stored in flash memory. This is used when the Agent is managing passwords locally (or initially for all cases on reboot). This is the SNMPv3 password used for Authentication (currently, only MD5 is supported). This string can be up to 30 alpha-numeric characters.

¥ **V3 Privacy Password** Privacy password stored in flash memory. Used when the SNMP Agent is managing passwords locally (or initially for all cases on reboot). This is the SNMPv3 password used for privacy (DES encryption). This string can be between 8 and 30 alpha-numeric characters.

- **SNMP Mode**—This specifies the mode of operation of the radio's SNMP Agent. The choices are: disabled, v1_only, v2_only, v3_only. v1-v2, and v1-v2-v3. If the mode is disabled, the Agent does not respond to any SNMP traffic. If the mode is v1_only, v2_only, or v3_only, the Agent responds only to that version of SNMP traffic. If the mode is v1-v2, or v1-v2-v3, the Agent responds to the specified version of SNMP traffic. [**v1-v2-v3**]

- **Trap Version**—This specifies what version of SNMP will be used to encode the outgoing traps. The choices are v1_traps, v2_traps, and v3_traps. When v3_traps are selected, v2-style traps are sent, but with a v3 header. [**v1 Traps, v2 Traps, v3 Traps**]
- **Auth Traps Status**—Indicates whether or not traps will be generated for login events to the transceiver. [**Disabled/Enabled; Disabled**]
- **SNMP V3 Passwords**—Determines whether v3 passwords are managed locally or via an SNMP Manager. The different behaviors of the Agent depending on the mode selected, are described in **SNMP Mode** above.
- **Trap Manager #1–#4**— Table of up to 4 locations on the network that traps are sent to. [**Any standard IP address**]

NOTE: The number in the upper right-hand corner of the screen is the SNMP Agent's SNMPv3 Engine ID. Some SNMP Managers may need to know this ID in order interface with the transceiver's SNMP Agent. The ID only appears on the screen when SNMP Mode is either v1-v2-v3 or v3_only.

3.5 RADIO CONFIGURATION

There are two primary data layers in the transceiver network—radio and data. Since the data layer is dependent on the radio layer working properly, configuration of the radio items should be reviewed and set before proceeding. This section explains the *Radio Configuration Menu*, (Figure 3-19 for AP, Figure 3-20 for Remote). The Configuration Menu is followed a secondary menu, the *Skip Zone Options*.

3.5.1 Radio Configuration Menu

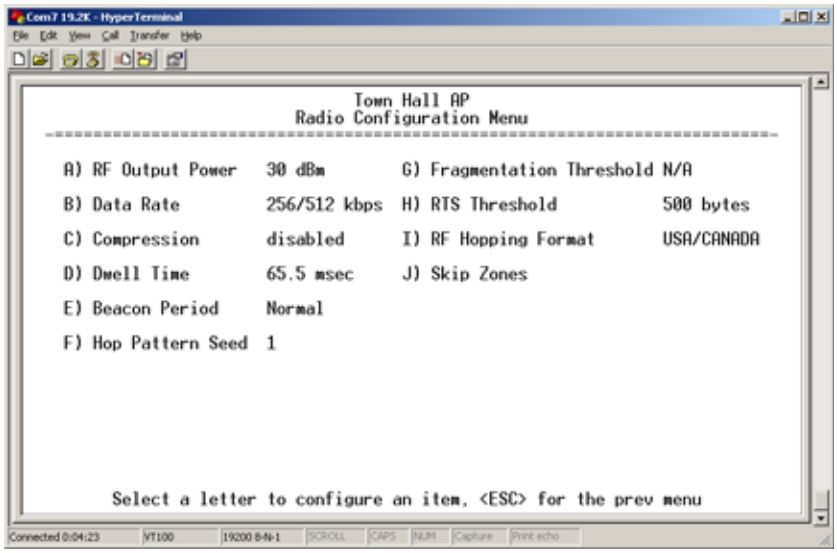


Figure 3-19. Radio Configuration Menu From *i*NET Access Point
(iNET II data rate selection is 512/1024 kbps)

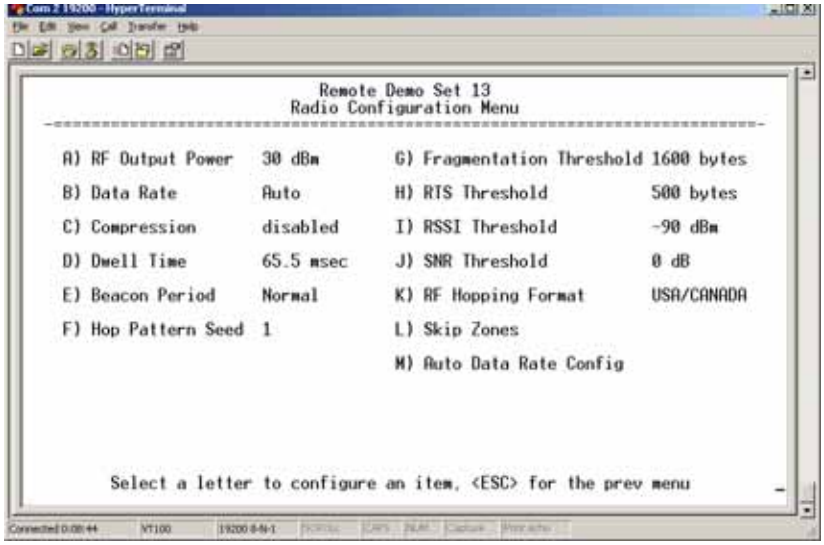

Remote Demo Set 13
Radio Configuration Menu
A) RF Output Power 30 dBm
B) Data Rate Auto
C) Compression disabled
D) Dwell Time 65.5 msec
E) Beacon Period Normal
F) Hop Pattern Seed 1
G) Fragmentation Threshold 1600 bytes
H) RTS Threshold 500 bytes
I) RSSI Threshold -90 dBm
J) SNR Threshold 0 dB
K) RF Hopping Format USA/CANADA
L) Skip Zones
M) Auto Data Rate Config
Select a letter to configure an item, <ESC> for the prev menu

Figure 3-20. Radio Configuration Menu
From Remote Unit

- **RF Output Power** *(User Review Recommended)*—Sets/displays RF power output level. Displayed in dBm. Setting should reflect local regulatory limitations and losses in antenna transmission line. (See *"How Much Output Power Can be Used?"* on Page 135 for information on how to calculate this value.) [**20–30; 20**]
- **Data Rate** (*Remote Only. AP fixed is at 256/512 kbps for iNET; 512/1024 kbps for iNET II.)*—Shows the over-the-air data rate setting for the Remote radio. Remotes can operate at one of two data rates when communicating with an AP; 256 kbps or 512 kbps (512 kbps or 1 Mbps for *i*NET II). 512 kbps data rates (1 Mbps for *i*NET II) are possible with strong RF signal levels, typically stronger than –77 dBm RSSI including a 15 dB fade margin.

  When the data rate is set to **AUTO**, the remote radio is able to change speeds based on the signal quality criteria set in the Auto Data Rate submenu described later in this section (see Page 52). [**256, 512, AUTO; AUTO**]

- **Compression** *(AP Only)*—Enabling this option uses LZO compression algorithm for over-the-air data. Varying levels of data reduction are achieved depending on the nature of the information. Text files are typically the most compressible, whereas binary files are the least compressible. On average, a 30% increase in throughput can be achieved with compression enabled.

- **Dwell Time** *(Not applicable to iNET II)*—Duration (in milliseconds) of one hop on a particular frequency in the hopping pattern. **Dwell Time** should be set to 32.8 ms. (This field is only changeable on an Access Point. Remotes get their value from AP upon association.)
[**16.4, 32.8, 65.5, 131.1, 262.1; 32.8**]

  TIP: If a packet is being transmitted and the dwell time expires, the packet will be completed before hopping to the next frequency.

- **Beacon Period** *(Not applicable to iNET II)*—Amount of time between Beacon transmissions (in msec).

  Available Intervals: **Normal** (104 ms), **Fast** (52 ms), **Faster** (26 ms), **Slow** (508 ms), **Moderate** (208 ms). These values provide relatively quick association times where Fast is very fast (≈ 5 sec) and the other end, the largest recommended value, the 508 ms period is slow (≈ 60 sec). [**Normal, Fast, Faster, Slow, Moderate; Normal**]

  TIP: Increasing the Beacon Period will provide a *small improvement* in network data throughput. Shortening it decreases the time needed for Remotes to associate with the AP. A short beacon period is usually only a benefit when there are mobile Remotes in the network.

- **Hop Pattern Seed** *(AP Only; Not applicable to iNET II)*—A user-selectable value to be added to the hop pattern formula. This is done in the unlikely event that identical hop patterns are used with two collocated or nearby networks. Changing the seed value will minimize the potential for RF-signal collisions in these situations. (This field is only changeable on an Access Point. Remotes read the AP's value upon association.) [**0 to 255; 1**]
- **Fragment Threshold**—Before transmitting over the air, if a packet exceeds this number of bytes, the transceiver sends the packet in multiple fragments that are reassembled before being delivered over the Ethernet interface at the receiving end. Only even numbers are acceptable entries for this parameter. Over-the-air data fragmentation is not supported on AP units. (See *"Network Performance Notes"* on Page 87 for additional information.)
[**256–1600 bytes; 1600**]

  TIP: In an interference-free environment this value should be large to maximize throughput. If interference exists then the value should be set to smaller values. The smaller the packet the less chance of it being interfered with at the cost of slightly reduced throughput.

- **RTS Threshold**—Number of bytes for the over-the-air RTS/CTS handshake boundary. (See *"Network Performance Notes"* on Page 87.) [**0 to 1600 bytes; 500**]

NOTE: While the transceiver accepts RTS Threshold values below 100, the lowest value that works is 100.

TIP: Lower the **RTS Threshold** as the number of Remotes or overall over-the-air traffic increases. Using RTS/CTS is a trade-off, giving up some throughput in order to prevent collisions in a busy over-the-air network.

The **RTS Threshold** should be enabled and set with a value smaller than the **Fragmentation Threshold** described above. RTS forces the Remotes to request permission from the AP before sending a packet. The AP sends a CTS control packet to grant permission to one Remote. All other Remotes stop transmitting for the specified amount of time.

- **RSSI Threshold (for alarm)**—Level (dBm) below which the received signal strength is deemed to have degraded, and a critical event (alarm) is generated and logged. Under these conditions, the PWR lamp flashes, and a trap is sent to the trap manager if SNMP is enabled and set properly. [**0 to -120; -90**]
- **SNR Threshold (for alarm)**—Value (dB) below which the signal-to-noise ratio is deemed to have degraded and a critical event is generated and logged. Under these conditions, the PWR lamp flashes, and a trap is sent to the trap manager if SNMP is enabled and set properly. [**0 to 40; Not Programmed**]
- **RF Hopping Format**—Operation compliant to country-specific restrictions into the frequency hopping algorithm. This option must be specified when the order is placed and cannot be modified in the field by the user. Authorizations at time of publication:
  - Australia: 915–928 MHz band
  - Brazil: 902-907.5 and 915-928 MHz bands
  - U.S.A. & Canada: 902–928 MHz band
  - Chile: 902–928 MHz, selectable hopping, from 1 to 80 channels
  - *i*NET II: Single-channel selectable from 2 to 79.

NOTE: Other country-specific configurations may be available. Check with your factory sales representative for new additions.

- **Skip Zones** *(Editable at AP Only)*—Display of current utilization of zones. Each zone consists of eight RF channels. In some instances there may be a part of the spectrum used by another system, that results in “continuous” or “persistent” interference to your system. To alleviate this form of interference, the transceiver may be programmed to “block out” affected portions of the spectrum using the Skip Zones Menu.

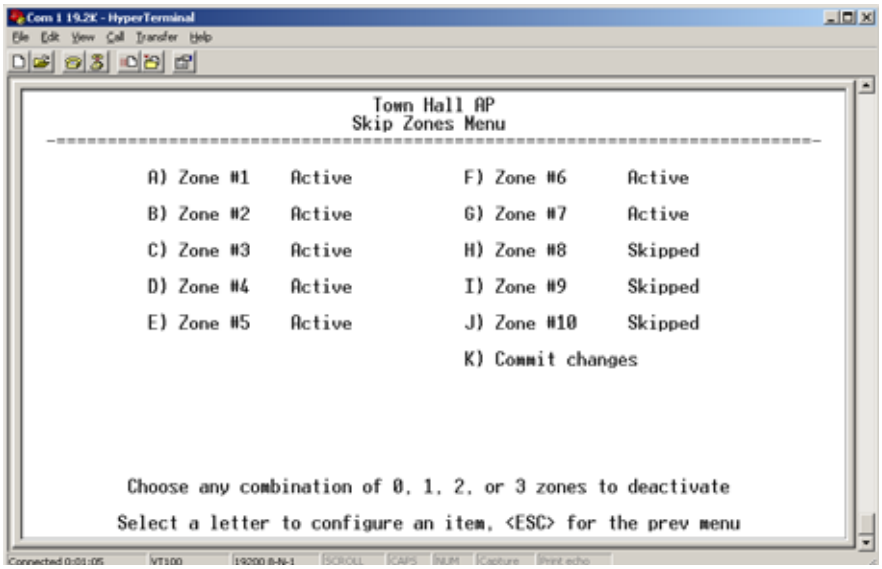

Com 1 19.2K - HyperTerminal
File Edit View Call Transfer Help
Town Hall AP
Skip Zones Menu
A) Zone #1 Active
B) Zone #2 Active
C) Zone #3 Active
D) Zone #4 Active
E) Zone #5 Active
F) Zone #6 Active
G) Zone #7 Active
H) Zone #8 Skipped
I) Zone #9 Skipped
J) Zone #10 Skipped
K) Commit changes
Choose any combination of 0, 1, 2, or 3 zones to deactivate
Select a letter to configure an item, <ESC> for the prev menu

Figure 3-21. Skip Zone Options Menu
("Commit changes" displayed only on Access Point units)

This is a display of current utilization of 10 zones, each of eight RF operating frequencies. Zones can be toggled between **Active** and **Skipped** at Access Point units by first keying in the letter of the zone to be changed, and then pressing the spacebar to toggle between the two options for each zone. Select the **Commit Changes** menu item to implement changes. These changes will be forwarded to all units in the network through the Access Point's beacon signal.

A maximum of three zones can be skipped and still be compliant with FCC regulations.

- **Auto Data Rate Configuration**—This selection brings up a submenu as shown in Figure 3-22. For the settings in this submenu to have any effect, the Data Rate menu item(Page 49) must be set to **AUTO.**

  The Auto Data Rate Configuration submenu is typically for use in environments where signal quality is variable, and you wish to maintain the highest possible over-the-air data rate as conditions change. Mobile applications are one example of where Auto Data Rate might be used.

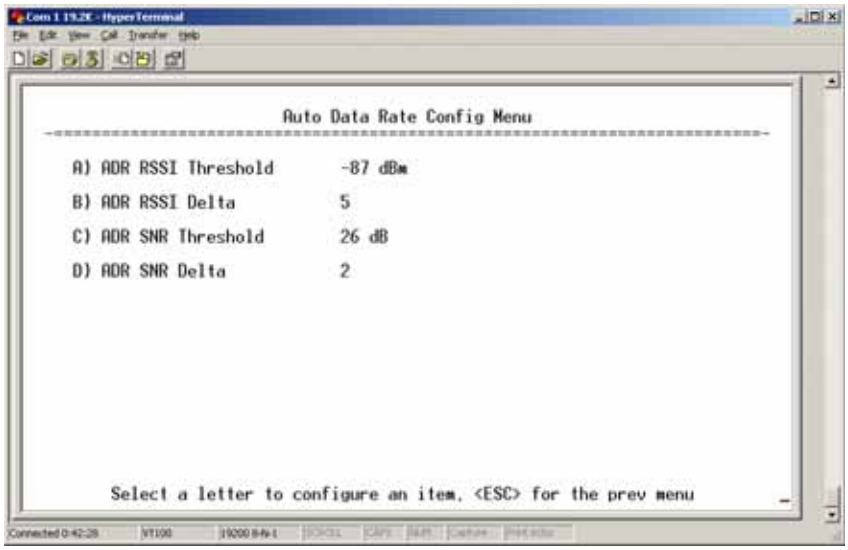

Com 1 19.2E - HyperTerminal
File Edit View Call Transfer Help
Auto Data Rate Config Menu
A) ADR RSSI Threshold -87 dBm
B) ADR RSSI Delta 5
C) ADR SNR Threshold 26 dB
D) ADR SNR Delta 2
Select a letter to configure an item, <ESC> for the prev menu
Connected 0:42:28
VT100

Figure 3-22. Auto Data Rate Menu

NOTE: In the description below, "high speed" refers to 512 kbps for the *i*NET radio and 1024 kbps for the *i*NET II radio.

"Standard speed" refers to 256 kbps for the *i*NET radio and 512 kbps for the *i*NET II.

The Auto Data Rate Configuration submenu consists of two threshold settings, each accompanied by a "delta" (amount of change) setting. Using the example of Figure 3-22, assume the current RSSI is -87 dBm. An RSSI reduction of more than 5 dBm (more negative RSSI number) would cause a data rate change from high speed to standard speed. Once the data speed has changed to standard speed, an RSSI *increase* to the level of -82 dBm would be required for the radio to switch back to high speed. This provides an operational "window" or hysteresis range over which the data speed stays constant despite minor changes in signal strength.

The SNR (signal-to-noise ratio) threshold and delta operate in the same manner described above, with the exception that the units are expressed in relative dB instead of dBm. In the example of Figure 3-22, a drop of 2 dB from a level of 26 dB would result in a data rate change from high speed to standard speed. For the radio to return to high speed, the SNR would need to increase to 28 dB. (*See Glossary for definition of SNR.)*

RSSI or SNR figures alone mean little when determining signal quality. Both parameters must be considered to get a true understanding of signal quality. For example, a strong, but noisy signal would likely be less useful than a weak signal with low noise levels. Proper use of the threshold and delta settings will result in smoother, more reliable performance from your wireless link.

Figure 3-22 shows the default values for RSSI and SNR parameters but these may be changed to optimize performance in your environment. In properly designed systems, experience has shown that RSSI levels between -50 dBm and -90 dBm provide reliable operation, provided the signal-to-noise ratio is 17 dB or above. Tailoring the thresholds with these baseline values in mind, can provide improved performance in your system.

The selections on the Auto Data Rate menu are as follows:

- **ADR RSSI Threshold**—A specified received signal strength value, which, if exceeded by the range of the **RSSI Delta** setting, causes a data rate change in the transceiver. [**-50 to -100**; **-87 dBm**]
- **ADR RSSI Delta**—A user-specified *difference* from the **RSSI Threshold** figure which, if exceeded, causes a data rate change in the transceiver. [**0-10**; **5**]
- **ADR SNR Threshold**—A user-specified signal-to-noise ratio, which, if exceeded by the range of the **SNR Delta** setting, causes a data rate change in the transceiver. [**10-30**; **26**]
- **ADR SNR Delta**—A user-specified *difference* from the **SNR Threshold** figure which, if exceeded, causes a data rate change in the transceiver. [**0-10**; **2**]

3.5.2 Mobile Data Configuration

Because a mobile environment is more demanding than fixed-site operation, additional considerations must be made at the time of configuration. These key points should be considered for all mobile installations:

- The use of middleware in the mobile laptops is important for the correct operation of a mobile data system. This software is not provided by MDS but is available from a number of vendors. Contact your MDS representative for suggested software.
- Configure the radios for mobile operation at the Remotes
- Set the Remote radios to standard speed (256 kbps for *i*NET, 512 kbps for *i*NET II) to optimize coverage
- Deploy Access Points so that they provide overlapping coverage
- Access Points must use the same network name to allow roaming

Enable and disable the mobility function using the Remote radio's Network Configuration Menu (see Figure 3-23). Although a menu selection appears in the Access Point's Network Configuration menu, this setting may not be changed there. When you enable the Remote radio's Mobility Mode option, the radio scans for an alternate AP if the RSSI is at or below the RSSI threshold defined in the Radio Configuration screen (see Figure 3-24).

After association is lost with an AP, and scanning for an alternate AP is started, the former AP is removed from the scan list for one minute, to

avoid linking back to the same AP. If no alternate AP is found, a link is eventually made to the same AP as before. This is why it is important to design a system with sufficient overlapping coverage by multiple APs.

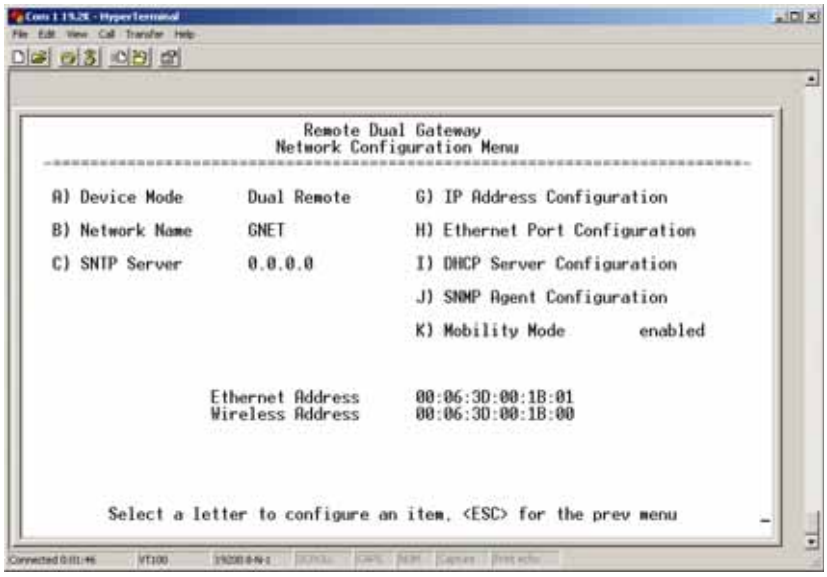

Remote Dual Gateway
Network Configuration Menu
A) Device Mode Dual Remote
B) Network Name GNET
C) SNTP Server 0.0.0.0
G) IP Address Configuration
H) Ethernet Port Configuration
I) DHCP Server Configuration
J) SNMP Agent Configuration
K) Mobility Mode enabled
Ethernet Address 00:06:3D:00:1B:01
Wireless Address 00:06:3D:00:1B:00
Select a letter to configure an item, <ESC> for the prev menu

Figure 3-23. Enabling Mobility at Remote Radio

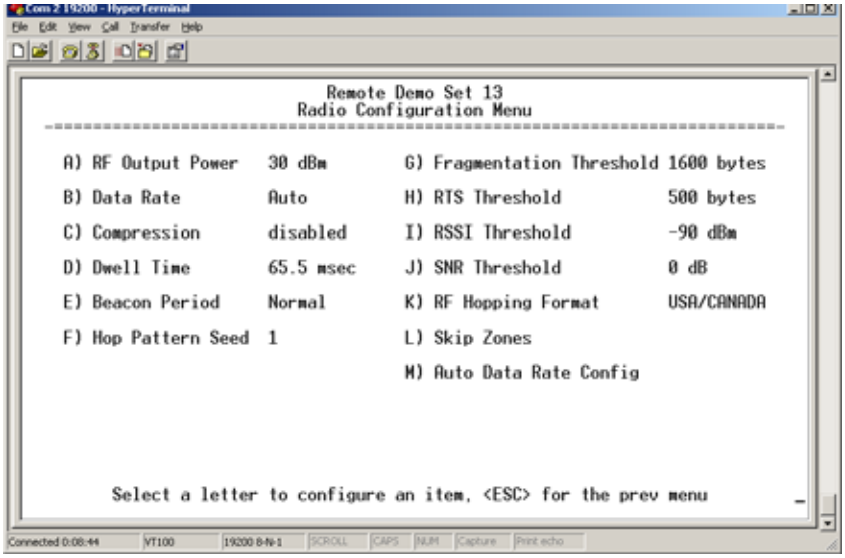

Remote Demo Set 13
Radio Configuration Menu
A) RF Output Power 30 dBm
B) Data Rate Auto
C) Compression disabled
D) Dwell Time 65.5 msec
E) Beacon Period Normal
F) Hop Pattern Seed 1
G) Fragmentation Threshold 1600 bytes
H) RTS Threshold 500 bytes
I) RSSI Threshold -90 dBm
J) SNR Threshold 0 dB
K) RF Hopping Format USA/CANADA
L) Skip Zones
M) Auto Data Rate Config
Select a letter to configure an item, <ESC> for the prev menu

Figure 3-24. Radio Configuration Screen—Remote

Other parameter settings that should be reviewed for Mobility Mode:

- **Compression** [**AP; disabled**]—Data compression is performed by the middleware running on the mobile laptop PC. Gains in efficiency are made because middleware compresses data at a higher stack level, and it aggregates multiple data frames and streams into a single packet. Compression at the radio level, although highly efficient, works at the individual packet level.

- **Dwell Time** [**AP; 16.4 milliseconds**]—This setting controls the amount of time that the unit spends on each frequency between hops. Due to the varying conditions of a mobile environment, this dwell time setting maximizes the benefits of frequency diversity. Although overall throughput appears to decrease by this setting, two benefits are gained: the effects of multipath fading are minimized through frequency diversity, and the compression described above compensates for the decreased throughput.
- **Beacon Period** [**AP; Fast**]—This parameter defines the interval at which the Access Point transmits a synchronization beacon to all remotes. This setting minimizes resynchronization times when remote radios roam between access points or in highly interrupted coverage areas (dense buildings, for example).
- **Fragmentation Threshold** [**remote; 256**]—This parameter defines the size of the message packets transmitted over the wireless media. These fragments are reconstructed into the original packet before delivery to the external device at the remote end of the link. In a mobile environment with rapidly changing conditions, setting this value to a minimum value improves the probability of packets being sent complete on the first try.
- **RTS Threshold** [**AP; 0 -1600 bytes**]—This setting is a wireless equivalent to RTS/CTS flow control in a normal communications circuit. This mechanism removes packet collisions caused by the "Hidden Node" scenario, in which remotes can't hear each other before transmitting. When this value is set below 100, it is essentially disabled.
- **Skip Zone Options**—In some instances there may be a part of the spectrum used by another system, that results in "continuous" or "persistent" interference to your system. To alleviate this form of interference, the transceiver may be programmed to "block out" affected portions of the spectrum using the Skip Zones Menu. This menu is fully described on Page 51.
- **Auto Data Rate**—The transceiver's Auto Data Rate feature can be very helpful in mobile environments, where signal quality tends to change rapidly. When signal quality is good, 512 kbps data speed can be used. If signal quality degrades, the radio automatically switches to 256 kbps. The criteria by which these speed changes will occur is controlled by the parameter settings in the Auto Data Rate Configuration submenu described on Page 52.

3.6 CONFIGURING THE SERIAL INTERFACES

3.6.1 Overview

The transceiver includes an embedded serial device server that provides transparent encapsulation over IP. In this capacity, it acts as a gateway

between serial and IP remote devices. Two common scenarios are PC applications using IP to talk to remote devices, and serial PC applications talking to remote serial devices over an IP network.

Essentially the same data services are available for both serial ports: COM1 and COM2. Note that the transceiver's COM1 port is DCE and COM2 is DTE. Therefore, if the RTU to be connected is also DTE, then a null-modem cable will need to be used when connecting to COM2.

NOTE: In the discussion that follows, COM1 and COM2 will be treated alike unless noted.

Com1 Port–*Dual Purpose Capability*

The COM1 port is used as a local console connection point and to pass serial data with an external device. Setting the COM1 port status to **Enable** prevents access to the Management System (MS) through this port. However, the MS can still be accessed via the LAN port using Telnet or a web browser.

To restore the COM1 port to support Management System services, connect a terminal to the port, select the proper baud rate (19,200 is default), and enter an escape sequence (**+++**) to reset it to the console mode.

TCP vs. UDP

Both types of IP services are used by the transceiver embedded serial device server—TCP and UDP. TCP provides a connection-oriented link with end-to-end acknowledgment of data, but with some added overhead. UDP provides a connectionless best-effort delivery service with no acknowledgment.

Most polled protocols will be best served by UDP service as the protocol itself has built-in error recovery mechanisms. UDP provides the needed multidrop operation by means of multicast addressing.

On the other hand, TCP services are best suited for applications that do not have a recovery mechanism (error-correction) and must have the guaranteed delivery that TCP provides despite the extra overhead. The IP-to-Serial example shows how to do this. (See *"IP-to-Serial Application Example"* on Page 67.)

Serial Encapsulation

Transparent encapsulation, or IP tunneling, provides a mechanism to encapsulate serial data into an IP envelope. Basically, all the bytes received through the serial port are put into the data portion of a TCP or UDP packet (TCP or UDP are user configurable options). In the same manner, all data bytes received in a TCP or UDP packet are output through the serial port.

When data is received by the radio through the serial port it is buffered until the packet is received completely. There are two events that signal an end-of-packet to the radio: a period of time since the last byte was received, or a number of bytes that exceed the buffer size. Both of these triggers are user configurable.

One radio can perform serial data encapsulation (IP-to-Serial) and talk to a PC. Two radios (or one radio and a terminal server) can be used together to provide a serial-to-serial channel.

TCP Client vs. TCP Server

On a TCP session there is a server side and a client side. The server is always waiting for requests from clients. The transceiver can be configured to act as either a server or a client.

The client mode attempts to establish a connection to a server (typically running on a PC) whenever it receives data on the serial port.

There is also a Client/Server mode where a connection is established in either the client or server modes. An incoming “keep alive” timer and outgoing counter

UDP Multicast

IP provides a mechanism to do a limited broadcast to a specific group of devices. This is known as “multicast addressing.” Many IP routers, hubs and switches support this functionality.

Multicast addressing requires the use of a specific branch of IP addresses set apart by the Internet Assigned Numbers Authority (IANA) for this purpose.

UDP multicast is generally used to transport polling protocols typically used in SCADA applications where multiple remote devices will receive and process the same poll message.

As part of the Multicast implementation, the radio sends IGMP membership reports and IGMP queries, and responds to membership queries. It defaults to V2 membership reports, but responds to both V1 and V2 queries.

You must configure the multicasted serial port as the target for the multicast data (for example, multipoint-to-multipoint mode, or point-to-multipoint mode where the inbound data is multicast). This restriction is because a host that only sends data to a multicast address (for example, point-to-multipoint mode where the *i*NET 900 acts as a point) will not join the group to receive multicast data because the host’s inbound data is directed unicast data.

The serial-to-serial example which follows shows how to provide multicast services. (See *"Point-to-Multipoint Serial-to-Serial Application Example"* on Page 69.)

PPP

External devices can connect to the transceiver using PPP (Point-to-Point Protocol). The transceiver works as a server and assigns an IP address to the device that connects through this interface.

To gain access to the transceiver from a PC even if the network is down, a modem may be connected to one of the transceiver's COM ports that has been configured with PPP.

Data Buffering

Data buffering is always active regardless of the selected mode. When Seamless mode is selected, a buffer size of 256 bytes is used. When custom mode is selected, the size options are: 16. 32, 64, 128, and 256 bytes. The Inter-Frame Delay is settable in either Seamless or Custom modes.

Implementing Configuration Changes

There are several configuration parameters for the Serial Gateway found under the *Serial Configuration Menu* of the Management System. After making changes to the configuration, you must use the menu's "Commit Changes" to assert the changes.

If you are connecting EIA-232 serial devices to the transceiver, review these parameters carefully.

Serial Configuration Wizard

The Serial Configuration Wizard available through the **Serial Gateway Configuration Menu** is recommended for configuration of serial ports. The wizard uses a step-by-step process, will eliminate possible conflicting settings, and streamline complex configurations.

The wizard can be bypassed by selecting option **B) View Current Settings** and adjusting the individual settings of the appropriate parameter

3.6.2 Serial Data Port Configuration Menu

The first two menu items present the identical parameter fields for each port with one exception—Flow Control. This is available only on COM2.

Serial Gateway
Serial Configuration Wizard
Welcome to the Serial Configuration Wizard. This wizard will assist you in the configuration of your available Serial Data Ports.
A) Begin Wizard
B) View Current Settings
Select a letter to choose item, 'Q' to quit wizard

Figure 3-25. Serial Configuration Wizard

- **Begin Wizard**—Tool for configuration of serial ports using a step-by-step process.
- **View Current Settings**—Displays all settable options. Depending on the selected IP protocol.

3.6.3 Configuring for UDP Mode

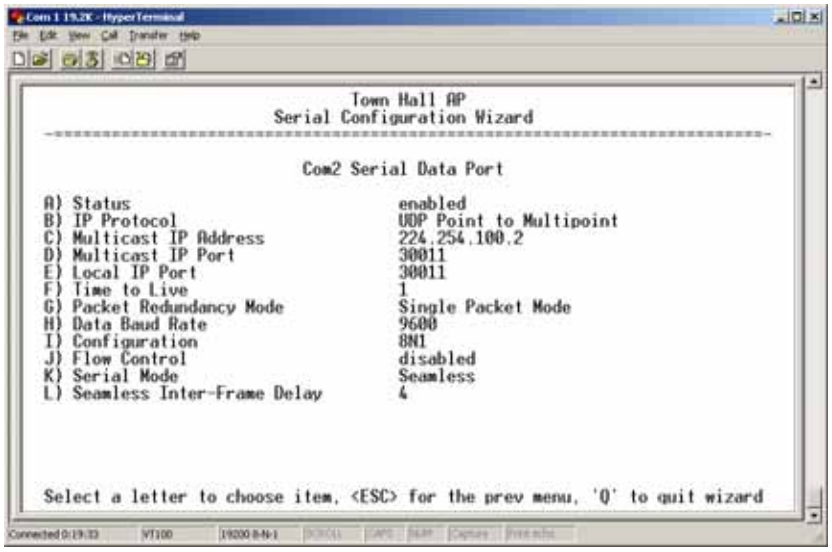

Town Hall AP
Serial Configuration Wizard
Com2 Serial Data Port
A) Status enabled
B) IP Protocol UDP Point to Multipoint
C) Multicast IP Address 224.254.100.2
D) Multicast IP Port 30011
E) Local IP Port 30011
F) Time to Live 1
G) Packet Redundancy Mode Single Packet Mode
H) Data Baud Rate 9600
I) Configuration 8N1
J) Flow Control disabled
K) Serial Mode Seamless
L) Seamless Inter-Frame Delay 4
Select a letter to choose item, <ESC> for the prev menu, 'Q' to quit wizard

Figure 3-26. UDP Point-to-Multipoint Menu

UDP point-to-multipoint to send a copy of the same packet to multiple destinations, such as in a polling protocol.

- **Status**—Enable/Disable the serial data port.

- **IP Protocol**—Point to Multipoint [**TCP, UDP PPP; TCP**]. This is the type of IP port that will be offered by the transceiver's serial device server.
- **Multicast IP Address** (used instead of **Local IP Address** when using UDP Point-to-Multipoint.)— Must be configured with a valid Class D IP address (224.0.0.0–239.255.255.255). IP packets received with a matching destination address will be processed by this unit [**Any legal IP address; 0.0.0.0**].
- **Multicast IP Port** (used instead of **Local IP Port** when using UDP Point-to-Multipoint.)—This port number must match the number used by the application connecting to local TCP or UDP socket. [**1-64,000; COM1: 30010, COM2: 30011**]
- **Local IP Port**—Receive IP data from this source and pass it through to the connected serial device. The port number must be used by the application connecting to local TCP or UDP socket. [**Any valid IP port; COM1: 30010, COM2: 30011**]
- **Time to Live (TTL)**—An IP parameter defining the number of hops that the packet is allowed to traverse. Every router in the path will decrement this counter by one.
- **Packet Redundancy Mode**— For proper operation, all radios' Serial Packet Redundancy mode must match (Single Packet mode vs. Packet Repeat mode). This is because a transceiver, when in Packet Repeat mode, sends 12 extra characters (sequence numbers, etc.) to control the delivery of the repeated data. Misconfigurations can result in undesired operation.
- **Data Baud Rate**—Data rate (payload) for the COM port in bits-per-second. [**1,200–115,200; 19200**]
- **Configuration**—Formatting of data bytes. Data bits, parity and stop bits [**7N1, 7E1, 7O1, 8N1, 8E1, 8O1, 8N1, 7N2, 7E2, 7O2, 8N2, 8E2, 8O2; 8N1**].
- **Flow Control [Com2 Only]**—RTS/CTS handshaking between the transceiver and the connected device. [**Enable, Disable; Disabled**]
- **Serial Mode**—When seamless mode is selected data bytes will be sent over the air as quickly as possible, but the receiver will buffer the data until enough bytes have arrived to cover worst-case gaps in transmission. The delay introduced by data buffering may range from 22 to 44 ms, but the radio will not create any gaps in the *output* data stream. This permits operation with protocols such as MODBUS™ that do not allow gaps in their data transmission. [**Seamless, Custom; Seamless**]
- **Seamless Inter-Frame Delay**— Number of characters that represent the end of a message (inter-character time-out). UDP packet sizes are delimited and sent out based on the Seamless Inter-Frame Delay only when receiving data through the serial port. MODBUS defines a "3.5-character" parameter. [**1–65,535; 4**]

- **Custom Data Buffer Size** (Custom Packet Mode only)—Maximum amount of characters, that the Remote end will buffer locally before starting to transmit data through the serial port. [**16, 32, 64, 128, 256; 32**]
- **Commit Changes and Exit Wizard**—Save and execute changes made on this screen (Shown only after changes have been entered.)

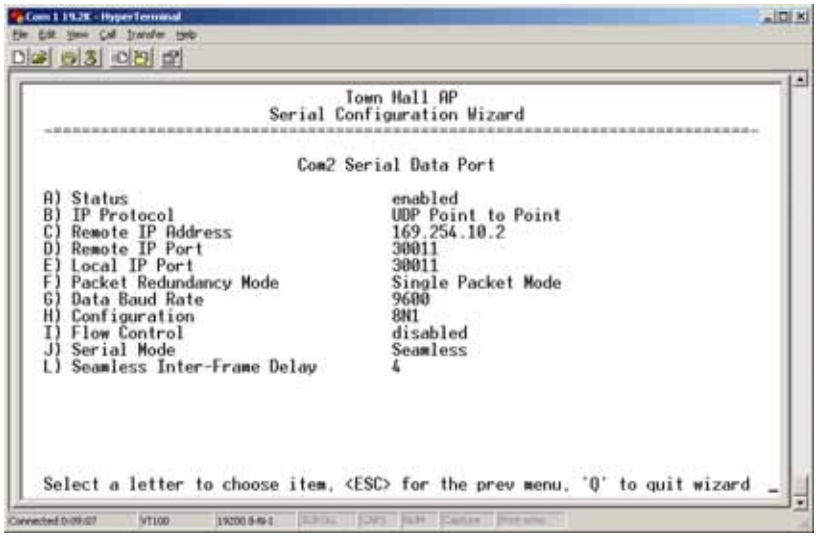

Town Hall AP
Serial Configuration Wizard
Com2 Serial Data Port
A) Status enabled
B) IP Protocol UDP Point to Point
C) Remote IP Address 169.254.10.2
D) Remote IP Port 30011
E) Local IP Port 30011
F) Packet Redundancy Mode Single Packet Mode
G) Data Baud Rate 9600
H) Configuration 8N1
I) Flow Control disabled
J) Serial Mode Seamless
L) Seamless Inter-Frame Delay 4
Select a letter to choose item, <ESC> for the prev menu, 'Q' to quit wizard

Figure 3-27. UDP Point-to-Point Menu

Use UDP point-to-point configuration to send information to a single device.

- **Status**—Enable/Disable the serial data port.
- **IP Protocol**—UDP Point-to-Point. This is the type of IP port that will be offered by the transceiver's serial device server. [**TCP, UDP, PPP; TCP**]
- **Remote IP Address**—Data received through the serial port is sent to this IP address. To reach multiple Remotes in the network, use UDP Point-to-Multipoint. [**Any legal IP address; 0.0.0.0**]
- **Remote IP Port**—The destination IP port for data packets received through the serial port on the transceiver. [**1–64,000; COM1: 30010, COM2: 30011**]
- **Local IP Port**—Port number where data is received and passed through to the serial port. This port number must be used by the application connecting to this transceiver. [**1–64,000; COM1: 30010, COM2: 30011**]

- **Packet Redundancy Mode**— For proper operation, all radios' Serial Packet Redundancy mode must match (Single Packet mode vs. Packet Repeat mode). This is because a transceiver, when in Packet Repeat mode, sends 12 extra characters (sequence numbers, etc.) to control the delivery of the repeated data. Misconfigurations can result in undesired operation.
- **Data Baud Rate**—Data rate (payload) for the COM port in bits-per-second. [**1,200–115,200; 19200**]
- **Configuration**—Formatting of data bytes. Data bits, parity and stop bits [**7N1, 7E1, 7O1, 8N1, 8E1, 8O1, 8N1, 7N2, 7E2, 7O2, 8N2, 8E2, 8O2; 8N1**].
- **Flow Control** (COM2 only)—RTS/CTS handshaking between the transceiver and the connected device. [**Enable, Disable; Disabled**]
- **Serial Mode**— When seamless mode is selected, data bytes will be sent over the air as quickly as possible, but the receiver will buffer the data until enough bytes have arrived to cover worst case gaps in transmission. The delay introduced by data buffering may range from 22 to 44 ms, but the radio will not create any gaps in the output data stream. This mode of operation is required for protocols such as MODBUS™ that do not allow gaps in their data transmission. [**Seamless, Custom; Seamless**]
- **Seamless Inter-Frame Delay**— Number of characters that represent the end of a message (inter-character time-out). MODBUS defines a "3.5-character" parameter. [**1–65,535; 4**]
- **Custom Data Buffer Size** (Custom Packet Mode only)—Maximum amount of characters, that the Remote end will buffer locally before starting to transmit data through the serial port. [**16, 32, 64, 128, 256; 32**]
- **Commit Changes and Exit Wizard**—Save and execute changes made on this screen (Shown only after changes have been entered.)

3.6.4 Configuring for TCP Mode

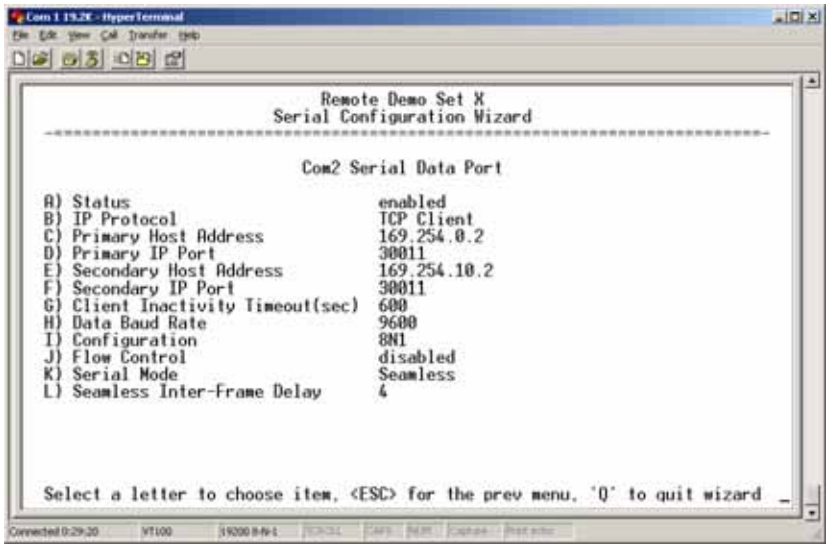

Com 1 19.2K - HyperTerminal
File Edit View Call Transfer Help
Remote Demo Set X
Serial Configuration Wizard
Com2 Serial Data Port
A) Status enabled
B) IP Protocol TCP Client
C) Primary Host Address 169.254.0.2
D) Primary IP Port 30011
E) Secondary Host Address 169.254.10.2
F) Secondary IP Port 30011
G) Client Inactivity Timeout(sec) 600
H) Data Baud Rate 9600
I) Configuration 8N1
J) Flow Control disabled
K) Serial Mode Seamless
L) Seamless Inter-Frame Delay 4
Select a letter to choose item, <ESC> for the prev menu, 'Q' to quit wizard
Connected 0:29:20
VT100
19200 8-N-1

Figure 3-28. TCP Client Menu (Remote)

- **Status**—Enable/Disable the serial data port.
- **IP Protocol**—TCP Client. This is the type of IP port that will be offered by the transceiver's serial device server. [**TCP, UDP, PPP; TCP**]
- **Primary Host Address**—The IP address to be used as a destination for data received through the serial port. [**Any legal IP address; 0.0.0.0**]
- **Primary IP Port**—The destination IP port for data packets received through the serial port on the transceiver. [**Any valid IP port; COM1: 30010, COM2: 30011**]
- **Secondary Host Address**—The IP address to be used as a destination for data received through the serial port in case the primary host address is not available. [**Any legal IP address; 0.0.0.0**]
- **Secondary IP Port**—The destination IP port for data packets received through the serial port on the transceiver used along with the secondary host address above. [**Any valid IP port; COM1: 30010, COM2: 30011**]
- **Outgoing Connection's Inactivity Timeout**—Amount of time (in seconds) that they transceiver will wait for data before terminating the TCP session. [**0–600; 600**]
- **Data Baud Rate**—Data rate (payload) for the COM port in bits-per-second. [**1,200–115,200; 19200**]
- **Configuration**—Interface signaling parameters. Data bits, parity and stop bits [**7N1, 7E1, 7O1, 8N1, 8E1, 8O1, 8N1, 7N2, 7E2, 7O2, 8N2, 8E2, 8O2; 8N1**].
- **Flow Control [Com2 Only]**—RTS/CTS handshaking between the transceiver and the connected device. [**Enable, Disable; Disabled**]

- **Serial Mode**— If data buffering is Enabled, the radio will operate in seamless mode. Data bytes will be sent over the air as quickly as possible, but the receiver will buffer the data until enough bytes have arrived to cover worst case gaps in transmission. The delay introduced by data buffering may range from 22 to 44 ms, but the radio will not create any gaps in the output data stream. This mode of operation is required for protocols such as MODBUS™ and some variants which do not allow gaps in their data transmission.
  [**Seamless, Custom; Seamless**]
- **Seamless Inter-Frame Delay**— Number of characters that represent the end of a message (inter-character time-out). MODBUS defines a "3.5-character" parameter.
  [**1–65,535; 4**]
- **Custom Data Buffer Size** (Custom Packet Mode only)—Maximum amount of characters, that the Remote end will buffer locally before starting to transmit data through the serial port.
  [**16, 32, 64, 128, 256; 32**]
- **Commit Changes and Exit Wizard**—Save and execute changes made on this screen (Shown only after changes have been entered.)

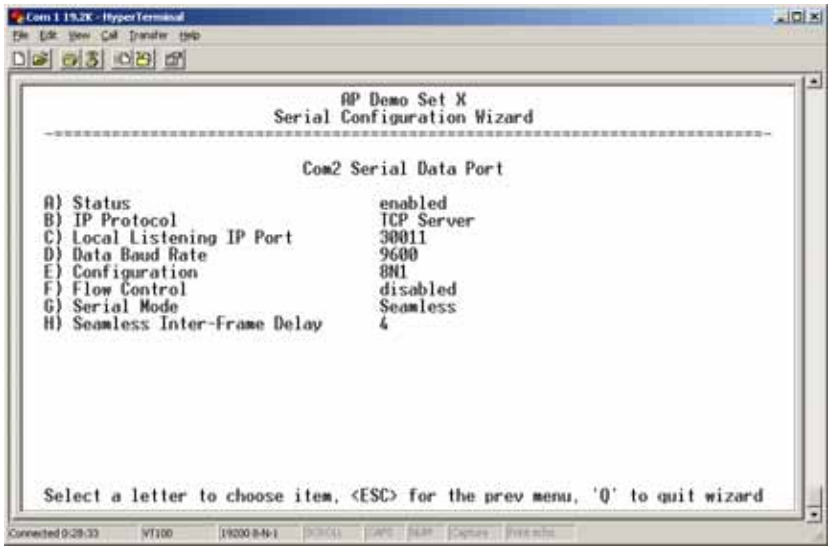

Com 1 19.2K - HyperTerminal
File Edit View Call Transfer Help
AP Demo Set X
Serial Configuration Wizard
Com2 Serial Data Port
A) Status enabled
B) IP Protocol TCP Server
C) Local Listening IP Port 30011
D) Data Baud Rate 9600
E) Configuration 8N1
F) Flow Control disabled
G) Serial Mode Seamless
H) Seamless Inter-Frame Delay 4
Select a letter to choose item, <ESC> for the prev menu, 'Q' to quit wizard
Connected 0:28:33
VT100
19200 8-N-1

Figure 3-29. TCP Server Menu (AP)

- **Status**—Enable/Disable the serial data port.
- **IP Protocol**—TCP Server. This is the type of IP port that will be offered by the transceiver's serial device server.
  [**TCP, UDP, PPP; TCP**]
- **Local Listening IP Port**—Receive IP data from this source and pass it through to the connected serial device. The port number must be used by the application connecting to local TCP or UDP socket.
  [**Any valid IP port; COM1: 30010, COM2: 30011**]

- **Data Baud Rate**—Data rate (payload) for the COM port in bits-per-second. [**1,200–115,200; 19200**]
- **Configuration**—Interface signaling parameters. Data bits, parity and stop bits
  [**7N1, 7E1, 7O1, 8N1, 8E1, 8O1, 8N1, 7N2, 7E2, 7O2, 8N2, 8E2, 8O2; 8N1**].
- **Flow Control** (COM2 only)—RTS/CTS handshaking between the transceiver and the connected device.
  [**Enable, Disable; Disabled**]
- **Serial Mode**— If data buffering is Enabled, the radio will operate in seamless mode. Data bytes will be sent over the air as quickly as possible, but the receiver will buffer the data until enough bytes have arrived to cover worst case gaps in transmission. The delay introduced by data buffering may range from 22 to 44 ms, but the radio will not create any gaps in the output data stream. This mode of operation is required for protocols such as MODBUS™ and some variants which do not allow gaps in their data transmission.
  [**Seamless, Custom; Seamless**]
- **Seamless Inter-Frame Delay**— Number of characters that represent the end of a message (inter-character time-out). MODBUS defines a "3.5-character" parameter. [**1–65,535; 4**]
- **Custom Data Buffer Size** (Custom Packet Mode only)—Maximum amount of characters, that the Remote end will buffer locally before starting to transmit data through the serial port. [**16, 32, 64, 128, 256; 32**]
- **Commit Changes and Exit Wizard**—Save and execute changes made on this screen (Shown only after changes have been entered.)

3.6.5 Configuring for PPP Mode

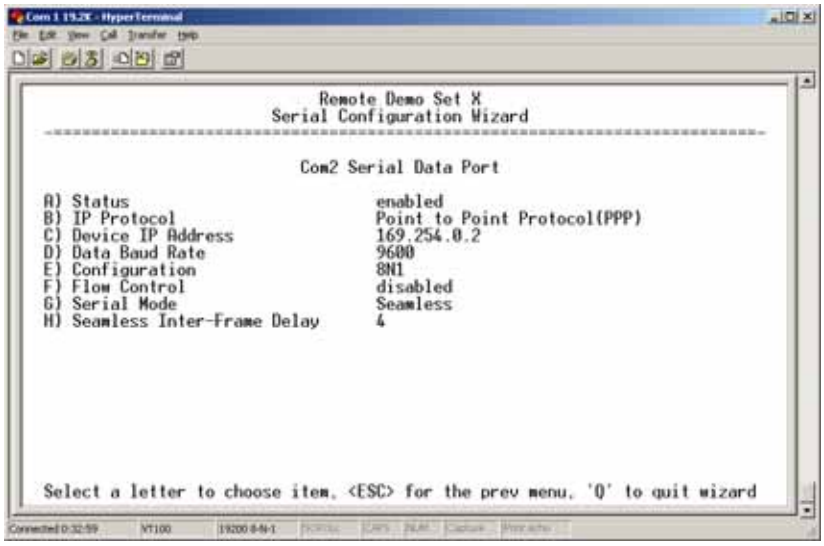

Remote Demo Set X
Serial Configuration Wizard
Com2 Serial Data Port
A) Status enabled
B) IP Protocol Point to Point Protocol(PPP)
C) Device IP Address 169.254.0.2
D) Data Baud Rate 9600
E) Configuration 8N1
F) Flow Control disabled
G) Serial Mode Seamless
H) Seamless Inter-Frame Delay 4
Select a letter to choose item, <ESC> for the prev menu, 'Q' to quit wizard

Figure 3-30. PPP Menu

- **Status**—Enable/Disable the serial data port.
- **IP Protocol**—PPP. This is the type of IP port that will be offered by the transceiver's serial device server. [**TCP, UDP, PPP; TCP**]
- **Device IP Address**—IP address that will be assigned to the dialing device once the connection is established. [**0.0.0.0**]
- **Data Baud**—The baud rate of the serial port of the transceiver to which the external device is connected. [**1200, 2400, 4800, 9600, 19200, 38400, 57600, 115200; 19200**]
- **Configuration**—Byte format of the serial port [**7N1, 7E1, 701, 7N2, 7E2, 702, 8N1, 801, 8N2, 8E2, 802; 8N1**]
- **Flow Control** (COM2 only)—RTS/CTS handshaking between the transceiver and the connected device. [**Enable, Disable; Disabled**]
- **Serial Mode**—When seamless mode is selected, data bytes will be sent over the air as quickly as possible, but the receiver will buffer the data until enough bytes have arrived to cover worst case gaps in transmission. The delay introduced by data buffering may range from 22 to 44 ms, but the radio will not create any gaps in the output data stream. This mode of operation is required for protocols such as MODBUS™ that do not allow gaps in their data transmission. [**Seamless, Custom; Seamless**]
- **Seamless Inter-Frame Delay**— Number of characters that represent the end of a message (inter-character time-out). MODBUS defines a "3.5-character" parameter. [**1–65,535; 4**]
- **Custom Data Buffer Size** (Custom Packet Mode only)—Maximum amount of characters, that the Remote end will buffer locally before starting to transmit data through the serial port. [**16, 32, 64, 128, 256; 32**]
- **Commit Changes and Exit Wizard**—Save and execute changes made on this screen (Shown only after changes have been entered.)

A PPP session shows the following possible states:

- **Sending LCP Requests**—The PPP server is querying for any clients that need to connect.
- **Link Established**—A successful PPP connection has been negotiated and an IP address is assigned.
- **Port not Enabled**—The serial port is disabled.

3.6.6 IP-to-Serial Application Example

You have a choice to use UDP or TCP to establish communications. This will depend on the type of device you are communicating with at the other end of the IP network. In this example we will use TCP to illustrate its use.

In TCP mode, the transceiver remains in a passive mode offering a socket for connection. Once a request is received, data received at the serial port will be sent out through the IP socket and vice versa, until the

connection is closed, or the link is interrupted. In this mode, the transceiver behaves the same, whether it is an Access Point or a Remote. (See Figure 3-31 and Table 3-1)

NOTE: The TCP session has a timeout of 10 minutes (600 seconds). If inactive for that time, it will be closed. The transceiver will offer the port again for connection after this time expires.

Establishing a Connection

From the PC, establish a TCP connection to the IP address of the Remote transceiver and to the IP port as configured above (30010—COM1, 30011—COM2). A Telnet client application can be used to establish this connection. Data can now be sent between the PC and the RTU or other connected device.

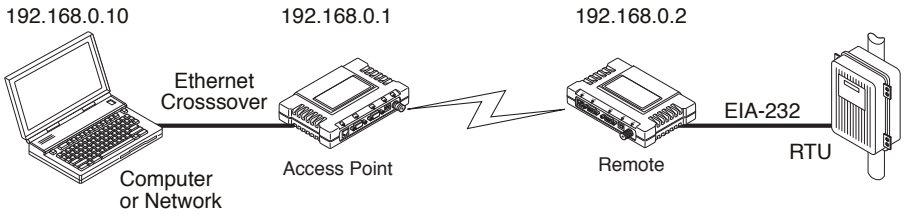


Figure 3-31. IP-to-Serial Application Diagram

Table 3-1. Serial Port Application Configuration

IP-to-Serial Connection

Transceiver Location	Menu Item	Setting
Access Point	None is required	None is required
Remote Unit	IP Address	192.168.0.2
	Status	Enabled
	IP Protocol	TCP
	Baud Rate	9,600 (Example)
	Flow Control	None
	Local IP Port	30011

3.6.7 Point-to-Point Serial-to-Serial Application Example

Once the transceivers are configured and the changes have been executed, they begin processing any data presented at the COM ports. Data presented at the Access Point's COM port will be packetized and sent via UDP to the Remote. Upon receiving the packet, the Remote strips the data out of the UDP packet and sends it out its COM port. Likewise, data presented at the Remote's COM port is packetized, sent to the Access Point, stripped, and sent out the Access Point's COM port. Note, this configuration does not use multicast addressing.

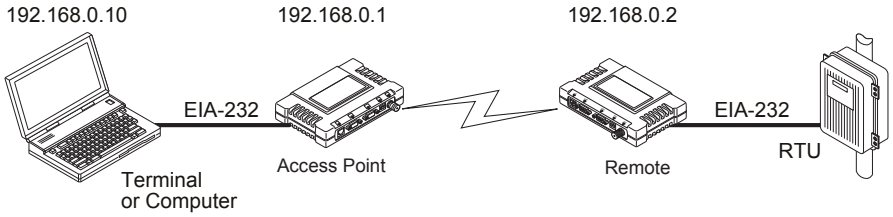


Figure 3-32. Point-to-Point Serial-to-Serial Application Diagram

Table 3-2. Serial Port Application Configuration

Transceiver Location	Menu Item	Setting
Access Point (COM2)[1]	Status	Enabled
	Data Baud Rate	9,600 (Example)
	Flow Control	Hardware (Example)
	Serial Mode	Seamless
	SIFD	4
	IP Protocol	UDP
	Remote IP Address	192.168.0.2 (IP address of the Remote radio)
	Remote IP Port	30011
	Local IP Port	30011
Remote Unit (COM2)[1]	Status	Enabled
	Data Baud Rate	9,600 (Example)
	Flow Control	X-ON/X-OFF (Example)
	Serial Mode	Seamless
	SIFD	4 (Characters)
	IP Protocol	UDP
	Remote IP Address	192.168.0.1 (IP address of the AP)
	Remote IP Port	30011
	Local IP Port	30011

1. Either COM port can be used, but they must be the same ones at both ends of the link. Both COM ports can be used simultaneously for two independent data channels.

3.6.8 Point-to-Multipoint Serial-to-Serial Application Example

The operation and data flow for this mode is very similar to Point-to-Point serial-to-serial application, except that it uses multicast addressing. The primary difference is that data presented at the Access Point's COM port will be packetized and sent via UDP to all of the Remotes. Upon receiving the packet all of the Remotes strip the data out of the UDP packet and send it out their COM port. Likewise, data presented at any of the Remotes' COM ports is packetized, sent to the

Access Point, stripped, and sent out the Access Point's COM port (see Figure 3-33, Table 3-3, Figure 3-34, and Figure 3-35 on Page 71.

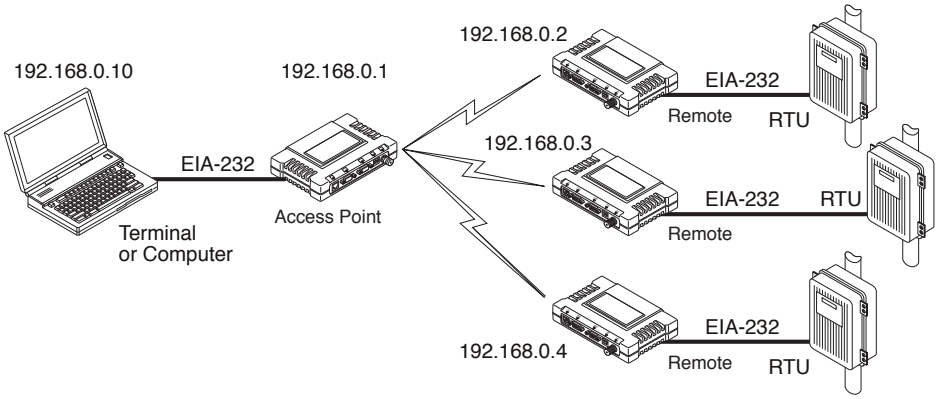


Figure 3-33. Point-to-Multipoint Serial-to-Serial Application Diagram

Table 3-3. Serial Port Application Configuration

Transceiver Location	Menu Item	Setting
Access Point (COM2)[1]	Status	Enabled
	Baud Rate	9600 (Example)
	Serial Mode	Custom
	Flow Control	Disabled
	IP Protocol	UDP
	Remote IP Address	224.254.1.1— Multicast Address[2]
	Remote IP Port	30011
	Local IP Port	30011
Remote Units (COM2)[1]	Enable	Enabled
	Baud Rate	2,400 (Example)
	Serial Mode	Custom
	Flow Control	Hardware (Example)
	IP Protocol	UDP
	Remote IP Address	192.168.0.1
	Remote IP Port	30011
	Local IP Port	30011
	Local Multicast Address	224.254.1.1 — Multicast Address[2]

1. Either COM port can be used, but they must be the same ones at both ends of the link. Both COM ports can be used simultaneously for two independent data channels.
2. This address is an example only. Any Class D IP address (224.0.0.0–239.255.255.255) will work.

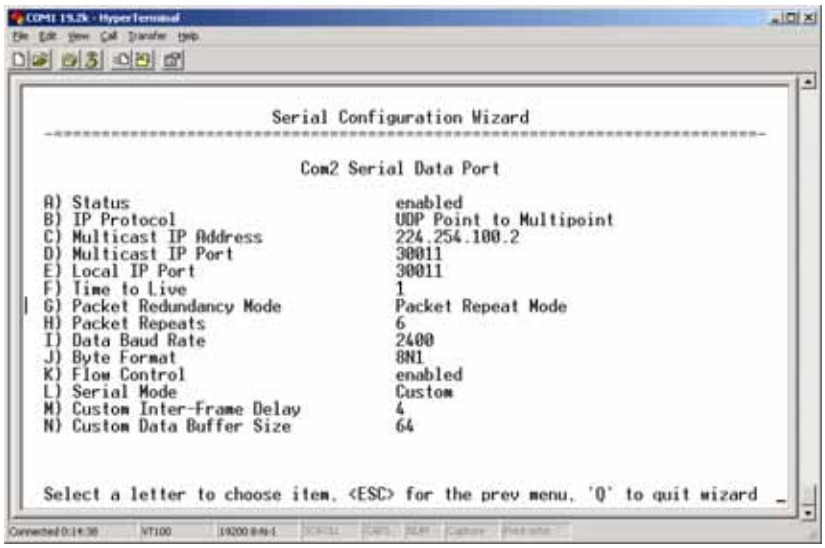

Serial Configuration Wizard
Com2 Serial Data Port
A) Status enabled
B) IP Protocol UDP Point to Multipoint
C) Multicast IP Address 224.254.100.2
D) Multicast IP Port 30011
E) Local IP Port 30011
F) Time to Live 1
G) Packet Redundancy Mode Packet Repeat Mode
H) Packet Repeats 6
I) Data Baud Rate 2400
J) Byte Format 8N1
K) Flow Control enabled
L) Serial Mode Custom
M) Custom Inter-Frame Delay 4
N) Custom Data Buffer Size 64
Select a letter to choose item, <ESC> for the prev menu, 'Q' to quit wizard

Figure 3-34. Access Point Serial Port Configuration

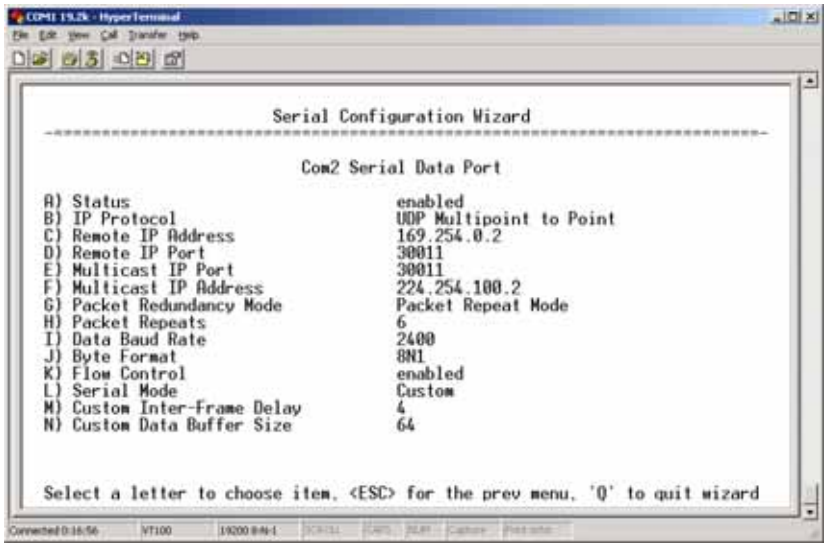

Serial Configuration Wizard
Com2 Serial Data Port
A) Status enabled
B) IP Protocol UDP Multipoint to Point
C) Remote IP Address 169.254.0.2
D) Remote IP Port 30011
E) Multicast IP Port 30011
F) Multicast IP Address 224.254.100.2
G) Packet Redundancy Mode Packet Repeat Mode
H) Packet Repeats 6
I) Data Baud Rate 2400
J) Byte Format 8N1
K) Flow Control enabled
L) Serial Mode Custom
M) Custom Inter-Frame Delay 4
N) Custom Data Buffer Size 64
Select a letter to choose item, <ESC> for the prev menu, 'Q' to quit wizard

Figure 3-35. Remote Radio Serial Port Configuration

3.6.9 Mixed Modes

Note that in this example, the TCP mode does not involve the Access Point. Thus, the transceiver in a single network can run in *both* modes at the same time. In other words, some Remotes can be configured for TCP mode while others can be configured (along with the Access Point) for UDP mode.

In this configuration, the Host PC can use both data paths to reach the RTUs. This may be helpful when a mixed collection of RTUs is present where some RTUs can operate in a broadcast form while others cannot (see Figure 3-36 on Page 72 and Table 3-4 on Page 72).

Operation and Data Flow

- Communicate with RTU A by Telneting to Remote 1, port 30011.
- Communicate with RTU B by Telneting to Remote 2, port 30011.
- Communicate with RTUs C and D by sending and receiving data from the Access Point's COM port.
- All communication paths can be used simultaneously.

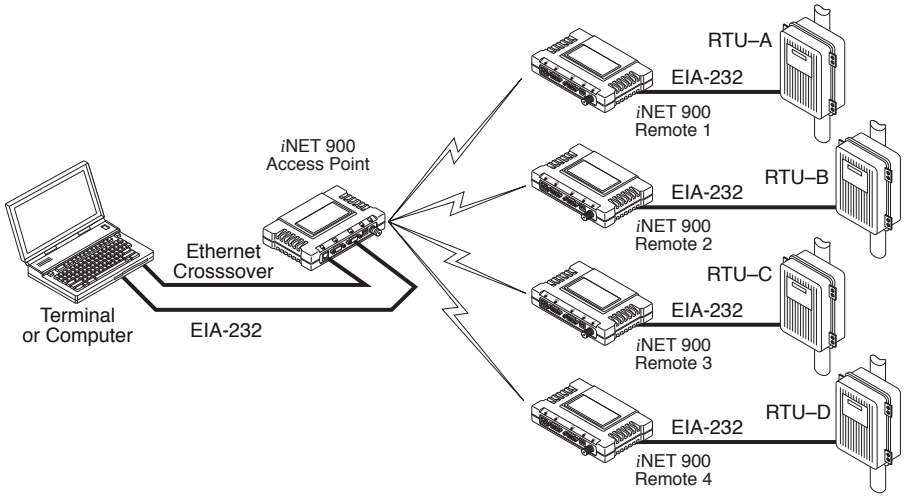


Figure 3-36. Mixed-Modes Application Diagram

Table 3-4. Serial Port Application Configuration

Transceiver Location	Menu Item	Setting
Access Point	Status	Enabled
	Baud Rate	9,600
	Flow Control	Disabled
	IP Protocol	UDP
	Send to Address	A multicast IP address such as 224.254.1.1
	Send to Port	30011
	Receive on Port	30011
	Receive on Address	0.0.0.0 (Not Used)
Remote Units 1 & 2 (COM2)	Status	Enabled
	Baud Rate	2,400
	Flow Control	Disabled
	IP Protocol	TCP
	Receive on Port	30011
Remote Units 3 & 4 (COM2)	Status	Enabled
	Baud Rate	9,600
	Flow Control	Disabled

Table 3-4. Serial Port Application Configuration *(Continued)*

Transceiver Location	Menu Item	Setting
	IP Protocol	UDP
	Send to Address	IP address of the AP
	Send to Port	30011
	Receive on Port	30011
	Receive on Address	224.254.1.1 (The multicast IP address used for the AP's Send To Address above)

3.7 SECURITY CONFIGURATION

There are many options to assist you in providing secondary security for your transceivers and the network. These options start with controlling remote access to the network via Telnet, Web Browser, and SNMP. Other areas include multiple levels of encryption and MD5-level security for HTTP connections.

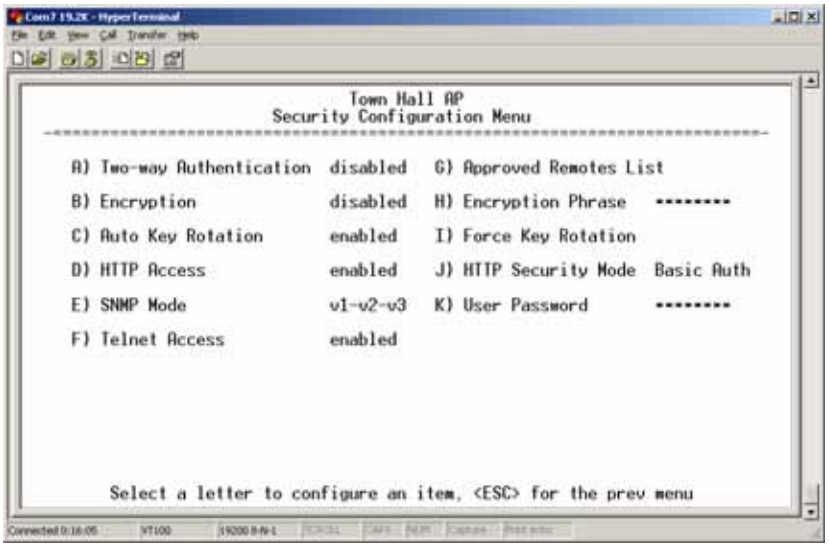

Town Hall AP
Security Configuration Menu
A) Two-way Authentication disabled
B) Encryption disabled
C) Auto Key Rotation enabled
D) HTTP Access enabled
E) SNMP Mode v1-v2-v3
F) Telnet Access enabled
G) Approved Remotes List
H) Encryption Phrase ********
I) Force Key Rotation
J) HTTP Security Mode Basic Auth
K) User Password ********
Select a letter to configure an item, <ESC> for the prev menu

Figure 3-37. Security Configuration Menu
(Access Point Version Shown)

- **Two-Way Authentication**— Enable provisioning at the Remote. [**Enabled/Disabled; Disabled**]

  Enabling forces the transceiver to check the *Approved AP List* before continuing the authorization process. In the case of a Remote, the AP must be in the *Approved Access Points List* before it accepts the beacon as valid. In the case of an AP, a Remote must be in the *Approved Remotes List* to be granted authorization. Before enabling this option, at least one entry must already exist in the *Approved List*.

- **Encryption**— Enable encryption of over-the-air data packets. [**Enabled, Disabled; Disabled**]

  Enabling forces the transceiver to use 128-bit encryption on all over-the-air messages. This option requires the Encryption Phrase to be previously configured.
- **Auto Key Rotation**—Enable automatic rotation of encryption keys. [**Enabled, Disabled; Disabled**]

  Enabling forces the transceiver to use the key rotation algorithm to generate a new encryption key after 500 kilobytes of information has been transmitted, or one hour has elapsed. Key rotation prevents reusing encryption data that could result in key-cracking, unlike standard 802.11b communications that rely on static encryption keys.
- **HTTP Access**—Prevents remote access through HTTP (Web browser) on Port 80 [**Enabled/Disabled; Disabled**]
- **SNMP Access**— Prevents remote access through SNMP commands on Port 161 [**Enabled, Disabled; Enabled**]
- **Telnet Access**—Prevents remote access through Telnet sessions on Port 23 [**Enabled, Disabled; Enabled**]
- **Approved Access Points/Remotes List** (Menu)—Go to menu providing the creation and management list of units permitted (provisioned) with which this unit will be permitted to communicate.
- **Encryption Phrase**—Phrase (text & numbers) that will be part of the encryption algorithm.
  [**Up to 29 alphanumeric characters; Blank**]
- **Force Key Rotation**— It triggers an immediate key rotation of the encryption keys before the internal counters do it automatically.
- **HTTP Security Mode**—Select security mode/level of login via HTTP browser. **HTTP Access** disabled prevents access through HTTP. **HTTP Security Mode** is functional if **HTTP Access** is enabled. [**Basic Auth, MD5 Digest; Basic Auth**]

  Basic mode requires a password, but the actual password text is transmitted in the clear (unencrypted).
- **User Password**—General administrative password only for this unit. Used at log-in via COM1 Port, Telnet and Web browser. [**Up to 8-character alphanumeric string without spaces (case-sensitive); admin**]

TIP: For enhanced security, consider using misspelled words, a combination of letters and numbers, and a combination of upper and lower case letters. Also, the password should use all eight characters. This helps protect against sophisticated hackers who may use a database of common words (for example, dictionary attacks) to determine a password.

3.7.1 Approved Remotes/Access Points List Menu

This menu is the same for both Access Points and Remotes and the names change to reflect their mode. Replace “Remotes” with Access Points” in the following description.

NOTE: The limit for remotes (in an Access Point) is 255. The limit for Access Points (in a remote) is 104.

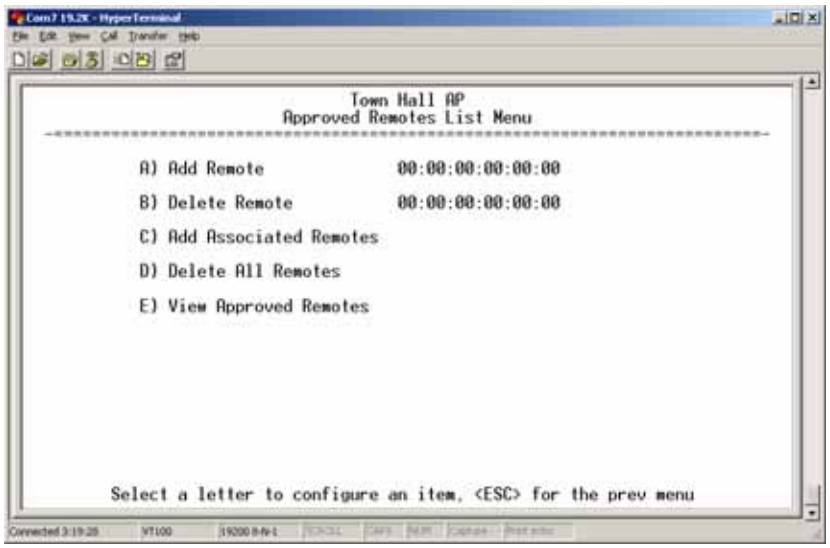

Town Hall AP
Approved Remotes List Menu
A) Add Remote 00:00:00:00:00:00
B) Delete Remote 00:00:00:00:00:00
C) Add Associated Remotes
D) Delete All Remotes
E) View Approved Remotes
Select a letter to configure an item, <ESC> for the prev menu

Figure 3-38. Approved Remotes List Menu

- **Add Remote**—Enter MAC address of Remote. [**Any valid 6-digit hexadecimal MAC address; 00:00:00:00:00:00**]
- **Delete Remote**—Enter MAC address of Remote.

  For security purposes, you may want to delete a stolen or deprovisioned radio.
- **Add Associated Remotes**—Add all currently associated remotes to the approved remote list. Alternatively, you can enter each Remote MAC manually.
- **Delete All Remotes**—Remove (complete purge) of all Remotes from current list.
- **View Approved Remotes**—Simple listing of approved Remotes by MAC address, of radios authorized to join this AP. If a Remote is not in this list, it will not be able to associate with this AP.
- **Save Changes**—Save all changes made during this session with this menu. Changes will be implemented only if they are “saved” before exiting this menu.

3.8 PERFORMANCE VERIFICATION

After the basic operation of the radio has been checked, you may wish to optimize the network's performance using some of the following suggestions. The effectiveness of these techniques will vary with the design of your system and the format of the data being sent.

There are two major areas for possible improvement—the radio and the data network. The following sections will provide you with a variety of items to check and on many occasions, ways to correct or improve their performance.

3.8.1 Performance Information Menu

This menu/screen is one of two primary sources of information on the radio layer and radio network performance.

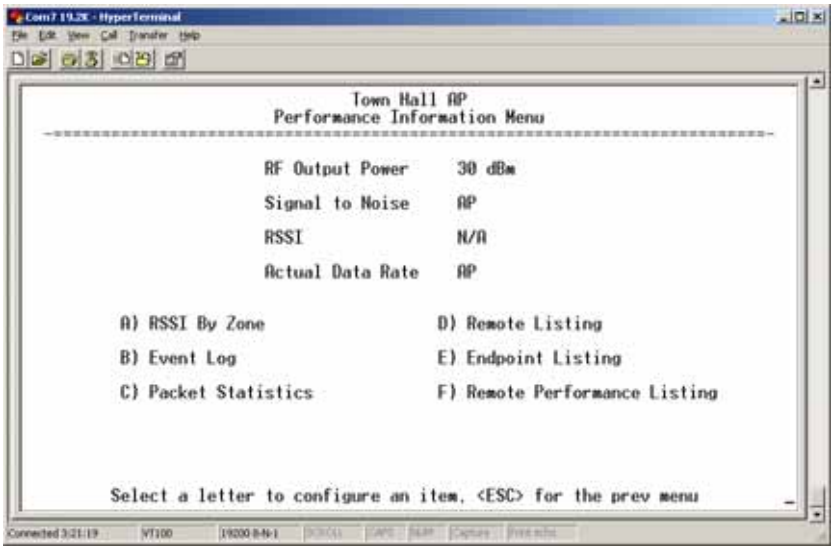

Com7 19.2E - HyperTerminal
Town Hall AP
Performance Information Menu
RF Output Power 30 dBm
Signal to Noise AP
RSSI N/A
Actual Data Rate AP
A) RSSI By Zone
B) Event Log
C) Packet Statistics
D) Remote Listing
E) Endpoint Listing
F) Remote Performance Listing
Select a letter to configure an item, <ESC> for the prev menu

Figure 3-39. Performance Information Menu
(AP Version Shown)

- **RF Output Power** *(Display only)*—Measured power output. (See *"How Much Output Power Can be Used?"* on Page 135)
- **Signal-to-Noise** *(Display only)*—Current running-average SNR value all active operating frequencies. (No value displayed on APs)
- **RSSI** *(Display only)*—Current running-average Received Signal Strength Indication for all active operating frequencies. (No value displayed on APs.)
- **Actual Data Rate** *(Display only)*—Over-the-air transmission rate (as opposed to selected data rate) for the remote being monitored. The fastest data rates can generally be achieved with stronger signal levels.
- **RSSI by Zone**—Received Signal Strength Indicator by Zone. (See *"RSSI by Zone Menu (Remotes Only)"* on Page 77)

- **Event Log**—Access the menu for managing the unit's log of operational activities.(See *"Authorization Key—Alter the unit's overall capabilities by enabling the built-in resources. (See "Authorization Keys Menu" on Page 105)"* on Page 91)
- **Packet Statistics**—Multiple radio and network operating statistics. (See *"Packet Statistics Menu"* on Page 81)
- **Wireless Network Status** *(Displayed only at Remotes)*—Current association state and MAC address of the Access Point. (See *"Wireless Network Status (Remotes Only)"* on Page 83)
- **Remote Listing** *(AP Display only)* —List of basic information for all Remote units currently associated with this Access Point. (See *"Remote Listing Menu (Access Points Only)"* on Page 84)
- **Endpoint Listing** *(AP Display only)*—List of units accessible by this AP through associated Remote ports. (See *"Endpoint Listing Menu (Access Points Only)"* on Page 85)
- **Remote Performance Listing** *(AP Display only)*—(See *"Remote Performance Listing Menu (Access Points Only)"* on Page 86)

RSSI by Zone Menu *(Remotes Only)*

This screen displays the strength of RF signals received from the currently associated Access Point.

Network integrity depends in large part on stable radio signal levels being received at each end of a data link. In general, signal levels stronger than –80 dBm will provide reliable communication that includes a 15 dB fade margin.

If you find there is a poor signal level on one zone, check the *Packet Statistics Menu* section on Page 81 and record the values. Then, set the questionable zone to "Skipped" in the Radio Configuration Menu (Page 48) and look for an improvement in the Packet Statistics error rates. If there is none, return the Zone to "Active."

RSSI measurements and Wireless Packet Statistics are based on multiple samples over a period of several seconds. The average of these measurements will be displayed by the Management System.

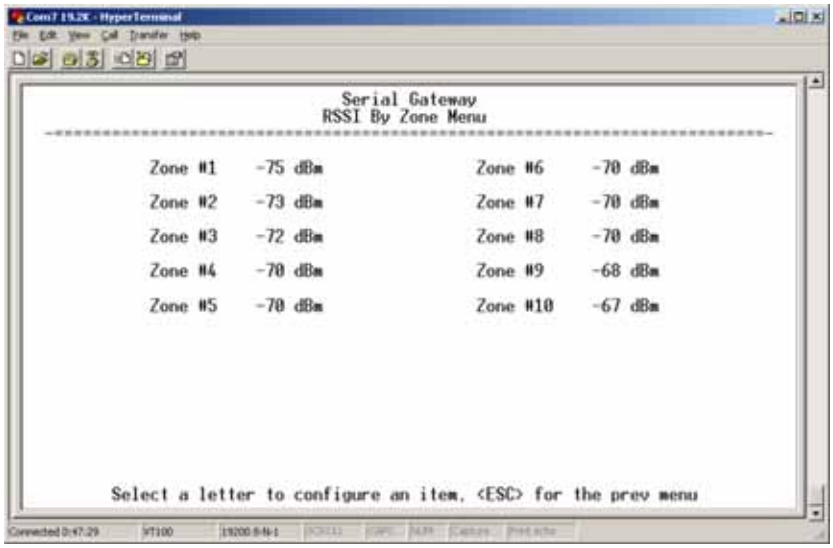

Serial Gateway
RSSI By Zone Menu
Zone #1 -75 dBm
Zone #2 -73 dBm
Zone #3 -72 dBm
Zone #4 -70 dBm
Zone #5 -70 dBm
Zone #6 -70 dBm
Zone #7 -70 dBm
Zone #8 -70 dBm
Zone #9 -68 dBm
Zone #10 -67 dBm
Select a letter to configure an item, <ESC> for the prev menu

Figure 3-40. RSSI by Zone Menu

TIP: Under normal circumstances, the signal levels in each zone should be within a few decibels of each other. If you see one that is significantly lower or higher, it may be a sign of radio frequency interference from another signal source on the 900 MHz band. See *"Network Performance Notes"* on Page 87 for further information.

Event Log Menu

The transceiver's microprocessor monitors many operational parameters and logs them. Events are classified into four levels of importance, which are described in Table 3-5. Some of these events will result from a condition that prevents the normal of the unit—these are "critical" events. These will cause the unit to enter an "alarmed" state and the PWR LED to blink until the condition is corrected. All events are stored in the Event Log that can hold up to 8,000 entries.

Table 3-5. Event Classifications

Level	Description/Impact
Informational	Normal operating activities
Minor	Does not affect unit operation
Major	Degraded unit performance but still capable of operation
Critical	Prevents the unit from operating

Time and Date

The events stored in the Event Log are time-stamped using the time and date of the locally connected device. Remote units obtain this information from the Access Point when they associate with it. The Access Point obtains the time and date from a Time Server. This server can generally be provided by a standard Windows PC server SNTP application. In the absence of the SNTP services, the user must manually enter it at the

Access Point. (See *"Device Information"* on Page 38 for SNTP server identification.) The manually set time and date clock is dependent on the unit's primary power. A loss of power will reset the clock to January 1, 2002 but will not affect previously stored error events.

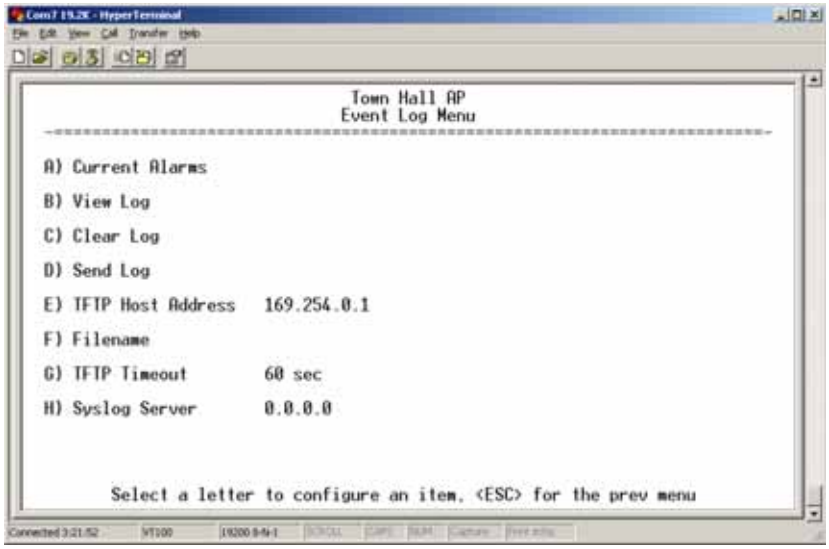

Town Hall AP
Event Log Menu
A) Current Alarms
B) View Log
C) Clear Log
D) Send Log
E) TFTP Host Address 169.254.0.1
F) Filename
G) TFTP Timeout 60 sec
H) Syslog Server 0.0.0.0
Select a letter to configure an item, <ESC> for the prev menu

Figure 3-41. Event Log Menu

- **Current Alarms** *(Telnet/Terminal only)*—View list of root causes that have placed the Device Status in the alarmed state. (See *"Alarm Conditions"* on Page 118)
- **View Log**—View a list of events stored in the current log. Some of these events are stored in volatile memory and will be erased with a loss of power. The events are numbered for easier identification and navigation.
- **Clear Log**—Purges the log of all events

  TIP: Save your Event Log before choosing to clear it in order to retain potentially valuable troubleshooting information. (See *"Upgrading the Firmware"* on Page 93 for an overview on how to transfer files from the transceiver to a computer on the network using TFTP.)

- **Send Log** *(Telnet/Terminal only)*—Initiate TFTP transfer of the unit's event Event Log in a plain text (ASCII) file to a TFTP server at the remote location.
- **TFTP Host Address** *(Telnet/Terminal only)*—IP address of the computer on which the TFTP server resides. This same IP address is used in other screens/functions (reprogramming, logging, etc.). Changing it here also changes it for other screens/functions. [**Any valid IP address; 127.0.0.1**]

- **Filename** *(Telnet/Terminal only)*—Name to be given to the Event Log file sent to the TFTP server for archiving. [**Any 40-char alphanumeric string; Blank**]

  NOTE: You may want to change the filename to reflect the type of log you intend to archive and/or its date.
- **TFTP Time-out** *(Telnet/Terminal only)*—Time in seconds the TFTP server will wait for a packet ACK (acknowledgment) from the transceiver before suspending the file transfer. [**10 to 120 seconds; 10**]
- **Syslog Server**—IP address to which alarms are sent using the syslog message format. [**Any valid IP address; 0.0.0.0**]

View Current Alarms

Most events, classified as "critical" will make the PWR LED blink, and will inhibit normal operation of the transceiver. The LED will remain blinking until the corrective action has been completed.

An alarm condition is different from a log event in the sense that an alarm is persistent in nature. That is, an alarm condition remains as an alarm until it has been cleared by correcting the cause (see Table 4-6 on Page 120 for corrective action).

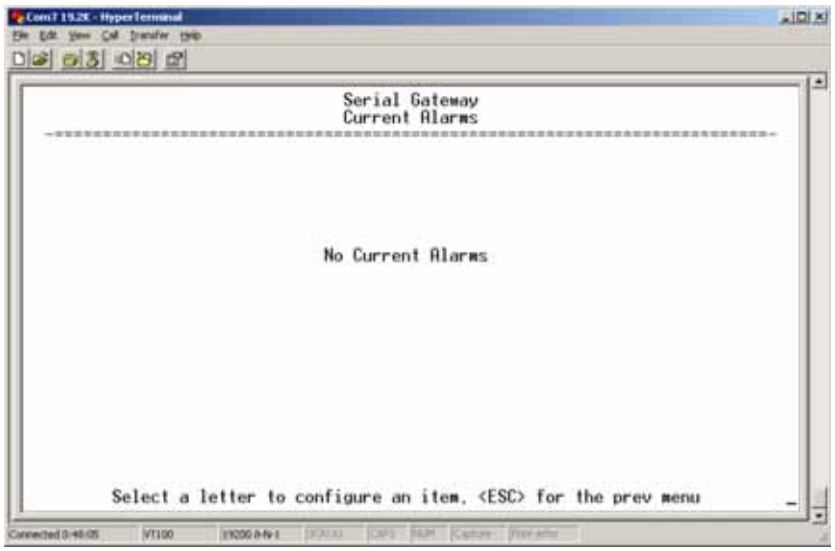


Figure 3-42. Current Alarms Screen

View Event Log

See Table 4-4 on Page 118 for event classifications.

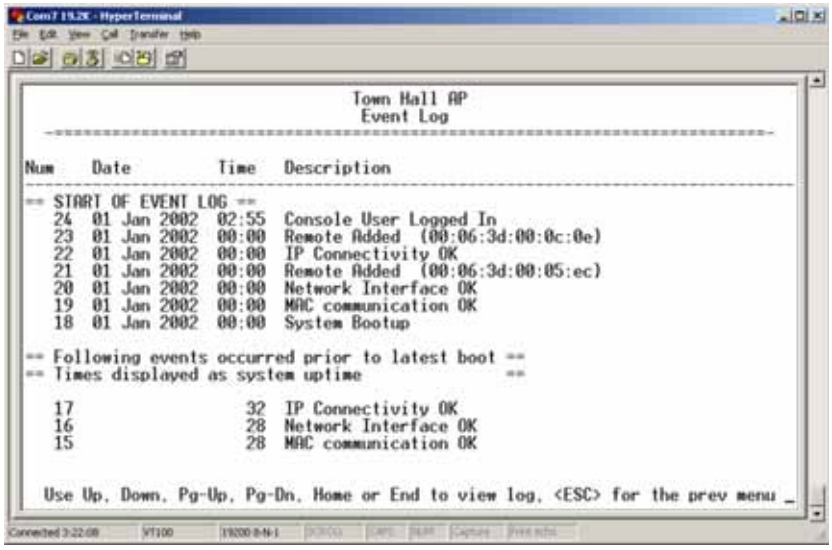

Town Hall AP
Event Log
Num Date Time Description
== START OF EVENT LOG ==
24 01 Jan 2002 02:55 Console User Logged In
23 01 Jan 2002 00:00 Remote Added (00:06:3d:00:0c:0e)
22 01 Jan 2002 00:00 IP Connectivity OK
21 01 Jan 2002 00:00 Remote Added (00:06:3d:00:05:ec)
20 01 Jan 2002 00:00 Network Interface OK
19 01 Jan 2002 00:00 MAC communication OK
18 01 Jan 2002 00:00 System Bootup
== Following events occurred prior to latest boot ==
== Times displayed as system uptime ==
17 32 IP Connectivity OK
16 28 Network Interface OK
15 28 MAC communication OK
Use Up, Down, Pg-Up, Pg-Dn, Home or End to view log, <ESC> for the prev menu

Figure 3-43. Sample Event Log Screen

Packet Statistics Menu

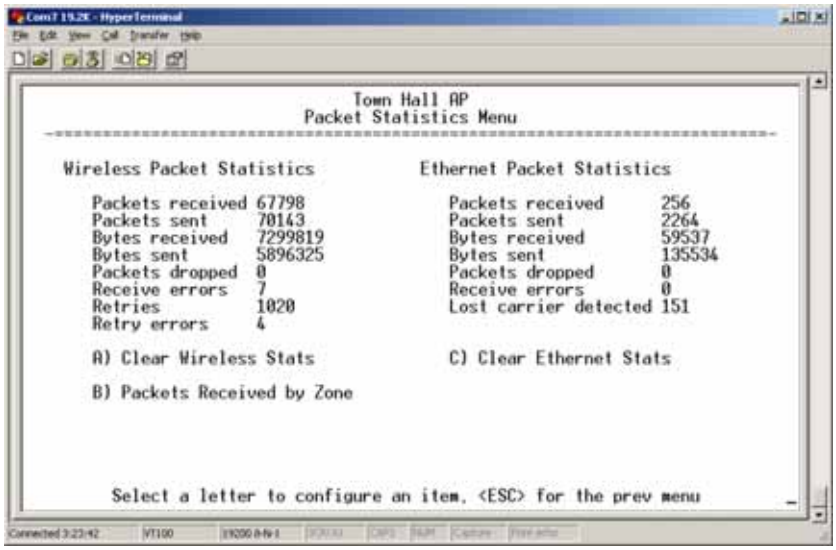


Figure 3-44. Sample Packet Statistics Menu

Wireless Packet Statistics

- **Packets received**—Over-the-air data packets received by this unit
- **Packets sent**—Over-the-air data packets sent by this Remote.
- **Bytes received**—Over-the-air data bytes received by this Remote.
- **Bytes sent**—Over-the-air data bytes sent by this Remote.
- **Packets dropped**—To-be-transmitted packets dropped as a result of a lack of buffers in the RF outbound queue.
- **Receive errors**—Packets that do not pass CRC. This may be due to transmissions corrupted by RF interference.

- **Retries**—Number of requests to re-send a data packet before it is acknowledged. If the packet was not acknowledged, this counter is not incremented.
- **Retry errors**—Packets discarded after exceeding seven retries over-the-air.
- **Clear Wireless stats**—Resets the statistics counter.

Ethernet Packet Statistics

- **Packets received**—Packets received by the transceiver through the Ethernet port.
- **Packets sent**—Packets transmitted by the transceiver through the Ethernet port.
- **Bytes received**—Data bytes received by this Remote through its LAN port.
- **Bytes sent**—Data bytes sent by this Remote.
- **Packets dropped**—Received packets dropped as a result of a lack of buffers.
- **Receive errors**—Packets that do not pass CRC. This may be due to collisions in the Ethernet LAN.
- **Lost carrier detected**—A count of the number of packets that the unit attempted to send out the Ethernet port when the carrier signal of the Ethernet was not present. (No carrier present could be due to a loose connection, bad or wrong cable, or equipment failure at the other end of the Ethernet cable.)
- **Clear Ethernet stats**—Resets the statistics counter.

Packets Received by Zone

This screen, shown in Figure 3-45, presents a breakdown of wireless packet statistics by-zone. All zones should report similar numbers. If one or more zones report lower numbers than the others (2% reduction), the specific zone is probably experiencing interference. An improvement can be realized by blocking this zone (see **Main Menu>>Radio Configuration>>Skip Zone Option**).

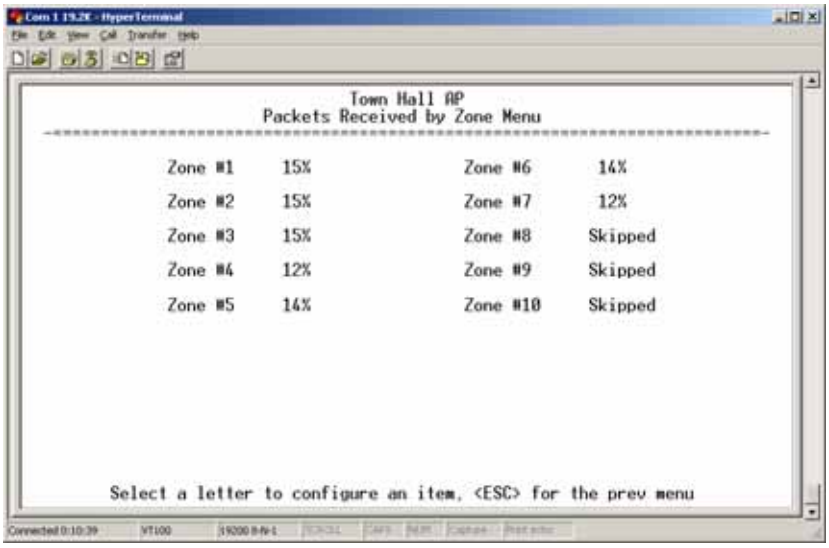


Figure 3-45. Packets Received By Zone Menu

Wireless Network Status

(Remotes Only)

The Wireless Network Status screen provides information on a key operating process of the transceiver—the association of the Remote with the Access Point. The following is a description of how this process takes place and as monitored on the *Figure 3-46. Wireless Network Status Screen"* on page 83.

The Transceiver's Association Process

After the Remote is powered up and finishes its boot cycle, it begins scanning the 900 MHz band for beacon signals being sent out from AP units. If the Remote sees a beacon with a *Network Name* that is the same as its own, the Remote will stop its scanning and temporarily synchronize its frequency-hopping pattern to match the one encoded on the AP's beacon signal. The Remote waits for three identical beacon signals from the AP and then it toggles into a fully synchronized "associated" state. If the Remote does not receive three identical beacons from the Access Point unit within a predetermined time period, it returns to a scanning mode and continues to search for an AP with a matching network name in its beacon.

Under normal circumstances, the association process should be completed within 20 seconds after boot-up. This time can vary depending on the beacon period setting at the AP. See **Beacon Period** description in Section 3.5.1, *Radio Configuration Menu* (beginning on Page 48).

Remote units are always monitoring the beacon signal. If an associated Remote loses the AP's beacon for more than 20 seconds, the association process starts again.

The Wireless Network Status Screen (Remote only)

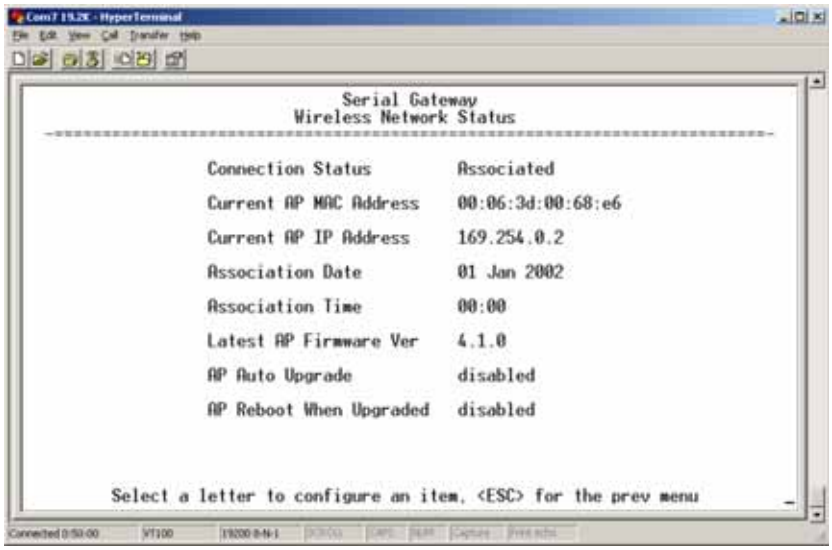

Serial Gateway
Wireless Network Status
Connection Status Associated
Current AP MAC Address 00:06:3d:00:68:e6
Current AP IP Address 169.254.0.2
Association Date 01 Jan 2002
Association Time 00:00
Latest AP Firmware Ver 4.1.0
AP Auto Upgrade disabled
AP Reboot When Upgraded disabled
Select a letter to configure an item, <ESC> for the prev menu

Figure 3-46. Wireless Network Status Screen

- **Connection Status**—Current state of the wireless network communication.

- *Scanning*—The unit is looking for an Access Point beacon signal.
- *Exp(ecting) Sync(hronization)*—The unit has found a valid beacon signal for its network.
- *Hop Sync*—The unit has changed its frequency hopping pattern to match that of the Access Point.
- *Associated* —This unit has successfully synchronized and associated with an Access Point. This is the normal status.
- *Alarmed*—The unit is has detected one or more alarms that have not been cleared.

- **Current AP Mac Address**—Wireless address of Access Point with which the Remote is associated.
- **Current AP IP Address**—IP address of Access Point with which the Remote is associated.
- **Association Date**—Date of last successful association with an Access Point.
- **Association Time**—Time of day association was established on the association date.
- **Latest AP Firmware Version**—
- **AP Auto Upgrade**—
- **AP Reboot when Upgraded**—

Remote Listing Menu *(Access Points Only)*

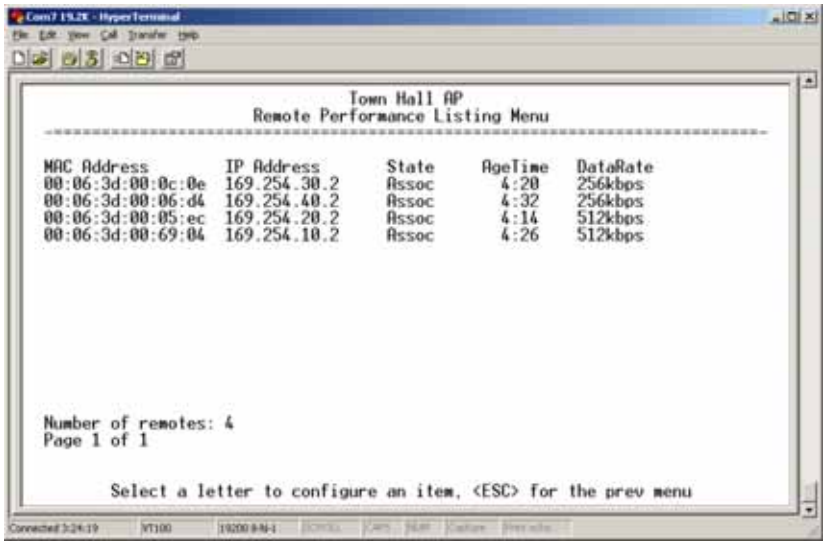

Town Hall AP
Remote Performance Listing Menu
MAC Address IP Address State AgeTime DataRate
00:06:3d:00:0c:0e 169.254.30.2 Assoc 4:20 256kbps
00:06:3d:00:06:d4 169.254.40.2 Assoc 4:32 256kbps
00:06:3d:00:05:ec 169.254.20.2 Assoc 4:14 512kbps
00:06:3d:00:69:04 169.254.10.2 Assoc 4:26 512kbps
Number of remotes: 4
Page 1 of 1
Select a letter to configure an item, <ESC> for the prev menu

Figure 3-47. Remote Listing Menu
(List of transceivers associated with this AP)

- **MAC Address**—Hardware address of the Remote transceiver.
- **IP Address**—IP Address of the Remote transceiver.
- **State**—Current association state of the Remote transceiver.
- **AgeTime**—Time, in minutes, remaining before the device (address) will be deleted from the table.

Each transceiver maintains a table with the addresses of the devices it communicates with. The age-time countdown is restarted to 5 minutes every time a message to/from that device is detected. If no traffic is exchanged with that device, it then "ages out" of the table. When traffic is detected it is included again in the table. This optimizes memory space utilization.

- **DataRate**—Supported data rate by this unit.

Endpoint Listing Menu

(Access Points Only)

This list shows all of the non-*i*NET 900 Ethernet devices that are known to the transceiver and is equivalent to the ARP table of IP devices.

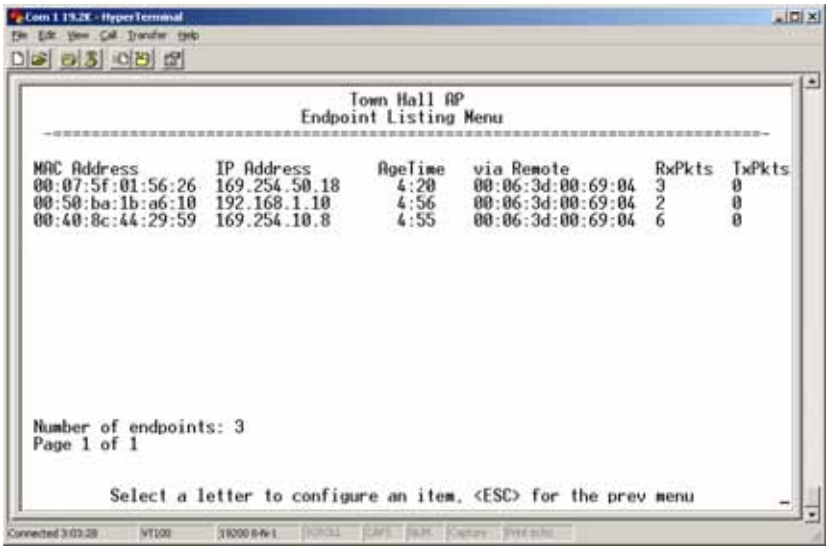

Town Hall AP
Endpoint Listing Menu
MAC Address IP Address AgeTime via Remote RxPkts TxPkts
00:07:5f:01:56:26 169.254.50.18 4:20 00:06:3d:00:69:04 3 0
00:50:ba:1b:a6:10 192.168.1.10 4:56 00:06:3d:00:69:04 2 0
00:40:8c:44:29:59 169.254.10.8 4:55 00:06:3d:00:69:04 6 0
Number of endpoints: 3
Page 1 of 1
Select a letter to configure an item, <ESC> for the prev menu

Figure 3-48. Endpoint Listing Menu
(Lists all equipment attached to REMOTE transceivers in the network)

- **MAC Address**—Hardware address of endpoint device.
- **IP Address**—IP Address of endpoint device.
- **AgeTime**—Time, in minutes, remaining before the device (address) will be deleted from the table.

  Each AP maintains a table with the addresses of the remote radios it communicates with. The age-time countdown is restarted to 5 minutes every time a message to/from that remote is detected. If no traffic is exchanged with that remote, it then "ages out" of the table. When traffic is detected it is included again in the table. This optimizes memory space utilization.
- **via Remote**—Hardware address of the transceiver connected to this device.
- **RxPkts**—Over-the-air data packets received by the transceiver. and passed on to the endpoint device.

- **TxPkt**—Number of packets received from the endpoint device and passed over-the-air.

Remote Performance Listing Menu
(Access Points Only)

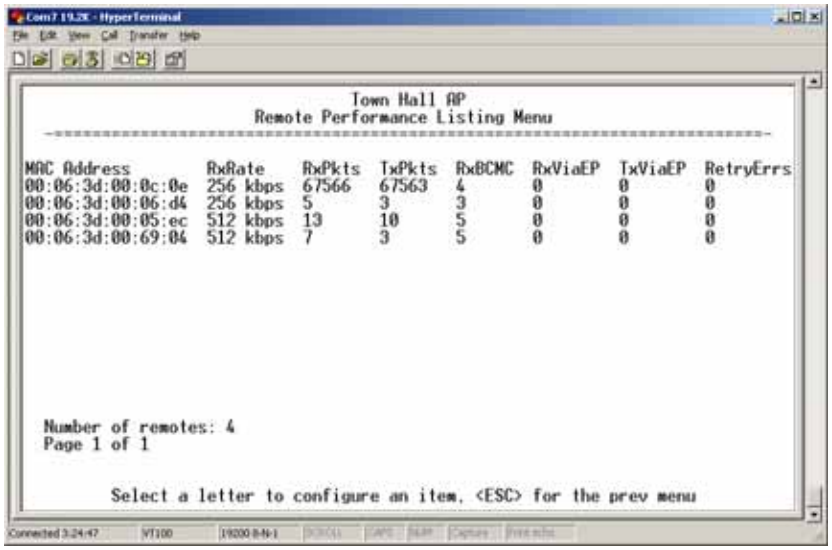

Town Hall AP
Remote Performance Listing Menu
MAC Address RxRate RxPkts TxPkts RxBCMC RxViaEP TxViaEP RetryErrs
00:06:3d:00:0c:0e 256 kbps 67566 67563 4 0 0 0
00:06:3d:00:06:d4 256 kbps 5 3 3 0 0 0
00:06:3d:00:05:ec 512 kbps 13 10 5 0 0 0
00:06:3d:00:69:04 512 kbps 7 3 5 0 0 0
Number of remotes: 4
Page 1 of 1
Select a letter to configure an item, <ESC> for the prev menu

Figure 3-49. Remote Performance Listing Menu for *i*NET AP
(iNET II will show RxRate as 512 kbps or 1024 kbps)

This screen provides a unit-by-unit summary of all Remote units currently associated with this Access Point. The parameters are displayed in a column format with each line corresponding to one Remote.

- **RxRate**—Over-the-air data rate the radio is currently using. All transceivers do not need to use the same rate.
- **RxPkts**—Over-the-air data packets received from this unit.
- **TxPkts**—Over-the-air data packets sent to this unit.
- **RxBCMC**—Total number of Broadcast and/or Multicast packets received over-the-air.
- **RxViaEP**—Packets received by the transceiver through the Ethernet port.
- **TxViaEP**—Packets sent by the transceiver through the Ethernet port.
- **RetryEr**—Packets discarded after exceeding five retries over-the-air.

Serial Data Statistics Menu

This screen provides a summary of port activity for both serial data ports. These values will be reset to zero after a reboot cycle.

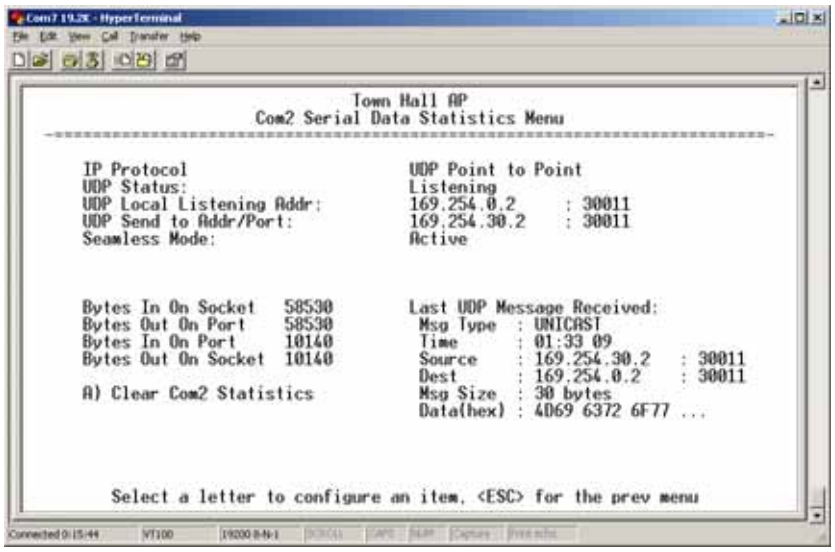


Figure 3-50. Serial Data Statistics Screen
(Both COM1 and COM2 will be shown)

- **Bytes in on port—**Number of bytes received by the transceiver through the serial interface
- **Bytes out on port—**Number of bytes transmitted by the transceiver through the serial interface
- **Bytes in on socket—**Number of bytes received by the transceiver through the IP socket
- **Bytes out on socket—**Number of bytes transmitted by the transceiver through the IP socket

  In general, the number of bytes **Out on Socket** should follow the number of bytes **In On Port** as all bytes received on the serial port should be transmitted out to the IP interface. The same should be true in the opposite direction, bytes **Out On Port** should follow bytes **In On Socket.**
- **Clear Com1 Statistics**—Resets counter to zero.
- **Clear Com2 Statistics**—Resets counter to zero.

3.8.2 Network Performance Notes

Principles of Network Operation

The following is a list of points that are useful for dealing with the networking aspects of the transceiver.

1. The transceiver serves as a network bridge.

- The radio goes through a listening and learning period at start-up before it will send any packets over either of its ports. This is about 10 seconds after the CPU's operating system has finished its boot cycle.
- The bridge code in the transceiver operates and makes decisions about packet forwarding just like any other bridge. The bridge code builds a list of source MAC addresses that it has seen on each of its ports.
  There are a few general rules that are followed when a packet is received on any port:
  - If the destination address is a multicast or broadcast address, forward the packet to all remotes.
  - If the destination address is not known, forward the packet to all remotes.
  - If the destination address is known, forward the packet to the port that the destination is known to be on (usually the RF port).
  - The bridge code uses Spanning Tree Protocol (STP) to prevent loops from being created when connecting bridges in parallel. For example, connecting two remotes to the same wired LAN could create a loop if STP was not used. Every bridge running STP sends out Bridge Protocol Data Units (BPDUs) at regular intervals so that the spanning tree can be built and maintained. BPDUs are 60-byte multicast Ethernet frames.

2. The wireless MAC has two settings that can be adjusted.

   - **Fragmentation threshold** is the threshold in bytes, which causes the MAC to fragment a packet.
   - **RTS threshold** is the threshold in bytes that causes the MAC to use RTS/CTS before sending the packet.

3. Because of timers and other components of the protocol, there is a maximum distance limit of 40 miles for reliable operation. Repeater stations may be used to extend this range.

4. Throughput calculations must take into account all overhead.

The following is an example of the overhead at each layer for a 100-bytes of data over UDP:

- Data: 100 bytes
- UDP header: 8 bytes
- IP header: 20 bytes
- Ethernet header: 14 bytes
- 802.11 header 24 bytes
- LLC and SNAP header: 8 bytes
- FHSS (*i*NET) header and FCS: 16 bytes

Total over-the-air frame size=190 bytes

If the frame is directed (for example: not multicast/broadcast), the 802.11 ACK frame must be accounted for:

- 14 bytes—802.11 ACK
- 30 bytes—Over-the-air ACK frame (added 16 the FHSS PHY)

If the 802.11 encapsulated Ethernet frame (NOT the UDP or Ethernet frame) exceeds the RTS threshold, then the overhead for RTS/CTS frames must also be accounted for.

- 20 bytes—802.11 RTS.
- 14 bytes—802.11 CTS.
- 66 bytes—Total Over-the-air bytes for RTS/CTS with PHY headers.

If the frame is TCP, then there is a 32-byte TCP header instead of the 8-byte UDP header.

- ARP requests, ARP replies and BPDU's will affect throughput.
- ARP requests are 60-byte Ethernet frames. 142 bytes over-the-air.
- ARP replies are 60-byte Ethernet frames. 142 bytes over-the-air.
- BPDUs are 60-byte Ethernet frames. 142 bytes over-the-air.

  Note that the overhead to put a single Ethernet frame over-the-air is 82 bytes. If RTS/CTS is invoked, it is 148 bytes. Therefore, the overhead for a minimal Ethernet frame (60 bytes) is 128% and, as such, gives the transceiver a poor small-packet performance.

If any radio in your network is connected to a large LAN, such as may be found in a large office complex, there may be undesired multi-cast/broadcast traffic over the air.

5. Station-to-Station Traffic

   - When sending frames from an endpoint connected to one transceiver to *another* endpoint with a different transceiver, the throughput will be halved at best. This is because all frames must go through the AP and thus are transmitted twice over the same radio system. Therefore, in the previous 100-byte UDP example, the number of over-the-air bytes will be 380 bytes (190 bytes x 2) if the frame has to go station-to-station.

6. Interference has a direct correlation to throughput.

   - Interference could be caused by any unnecessary traffic on the network from unrelated activities, or Radio Frequency Interference in the wireless spectrum.

Tips for Optimizing Network Performance

Here are some suggestion on things to try that may maximize throughput:

1. *AP Only:* Increment the **Dwell Time** to the maximum of 262.1 ms. This lowers the overhead since it will stay longer on a channel. The down side is that if a particular channel is interfered with it will take longer to hop to another channel.
   (**Main Menu>>Radio Configuration>>Dwell Time**)

2. *AP Only:* Change the **Beacon Period** to **Normal** (508 ms). This will also reduce the overhead of beacons sent out. On the down side, association time may be a little longer.
   (**Main Menu>>Radio Configuration>>Beacon Period**)

3. Change the **Fragmentation Threshold** to the maximum of 1600. Longer packets will be sent over the air reducing overhead. On the down side, if a packet is corrupted it will take longer to be retransmitted.
   (**Main Menu>>Radio Configuration>>Fragmentation Threshold**)

4. Increase the **RTS Threshold** to 1600. RTS mechanism is used to reserve a time slot if packets exceed this number. On the down side, a hidden-node might interfere more often than if RTS is not used.
   (**Main Menu>>Radio Configuration>>RTS Threshold**)

5. Decreasing the **RTS Threshold**, to the 100 to 200 range, will improve throughput on a busy network. It will add small packets, but reduce collisions (and resulting re-tries) of large packets.
   (**Main Menu>>Radio Configuration>>RTS Threshold**)

6. Use the **Performance Information Menu** to check the packets received by zone. (Remotes Only: **Main Menu>>Performance Information>>Packet Statistics>>Packets Received by Zone**)

   Readings should be close in value. A significantly lower value (2% reduction) probably indicates interference. Performance can be improved by blocking the affected zones at the Access Point. (**Main Menu>>Radio Configuration>>Skip Zone Option**)

7. Use the **Performance Information Menu** to check for errors, retries and dropped packets. Do the same with Ethernet traffic.

   With weak signals, interference, or hidden nodes, the optimal performance may be lower due to collisions and retries.

Data Latency—TCP versus UDP Mode

The latency of data passing through a network will depend on user data message length, the overall level of traffic on the network, and the quality of the radio path.

Under ideal conditions—low traffic and good RF signal path—the latency for units operating in the TCP mode, will typically be around 5 ms in each direction. However, when UDP multicast traffic is transported, the outbound packet latency (from AP to remote) is dependent on the beacon period.

UDP multicast packet latency can be minimized by setting the **Beacon Period** to **Fast** (52 ms). Changing beacon rate to **Fast** will result in an average latency of 31 ms, assuming outbound packets wait for a beacon transmission 50% of the time (26ms) plus the normal packet latency (5 ms).

Data Compression

Enabling this option uses an LZO compression algorithm for over-the-air data. Varying levels of data reduction are achieved depending on the nature of the data. Text files are typically the most compressible, whereas binary files are the least compressible. On average, a 30% increase in throughput can be achieved with compression enabled.

Compression is used on data packets of 100 bytes or more, including Ethernet, IP, and TCP/UDP headers.

3.9 MAINTENANCE

In the normal course of operating a wireless network, you will want to take advantage of product improvements, and to read and archive the configuration of your individual transceivers using the *Maintenance Menu*. This section provides detail information on how to take advantage of these services.

The maintenance tasks are:

- **Reprogramming**— Managing and selecting the unit's operating system firmware resources. *(See "Reprogramming Menu"* on Page 92*)*
- **Configuration Scripts**—Saving and importing data files containing unit operating parameters/settings. *(See "Configuration Scripts Menu"* on Page 97*)*
- **Authorization Key**—Alter the unit's overall capabilities by enabling the built-in resources. (*See "Authorization Keys Menu"* on Page 105*)*
- **Auto-Upgrade/Remote-Reboot**—Configure when remotes retrieve new firmware versions from the associated AP, and whether or not they reboot to the new firmware after receiving the new firmware. (See *"Auto-Upgrade/Remote-Reboot Menu"* on Page 106)
- **Radio Test**—A diagnostic tool for testing RF operation. (See *"Radio Test Menu"* on Page 107)

- **Ping Utility**—Diagnostic tool to test network connectivity. (See *"Ping Utility Menu"* on Page 108)

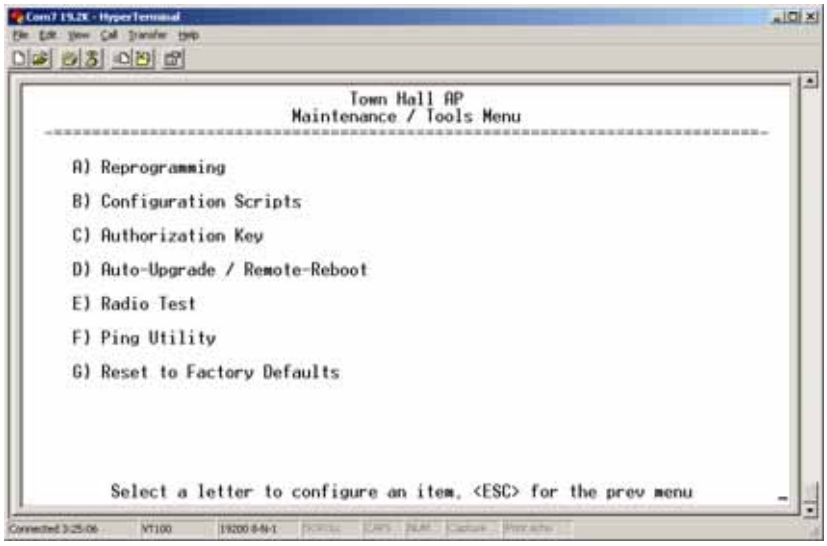

Town Hall AP
Maintenance / Tools Menu
A) Reprogramming
B) Configuration Scripts
C) Authorization Key
D) Auto-Upgrade / Remote-Reboot
E) Radio Test
F) Ping Utility
G) Reset to Factory Defaults
Select a letter to configure an item, <ESC> for the prev menu

Figure 3-51. Maintenance Menu

3.9.1 Reprogramming Menu

The transceiver has two copies of the firmware (microprocessor code) used for the operating system and applications. One copy is "active" and the second one is standing by, ready to be used. You can load new firmware into the inactive position and place it in service whenever you desire.

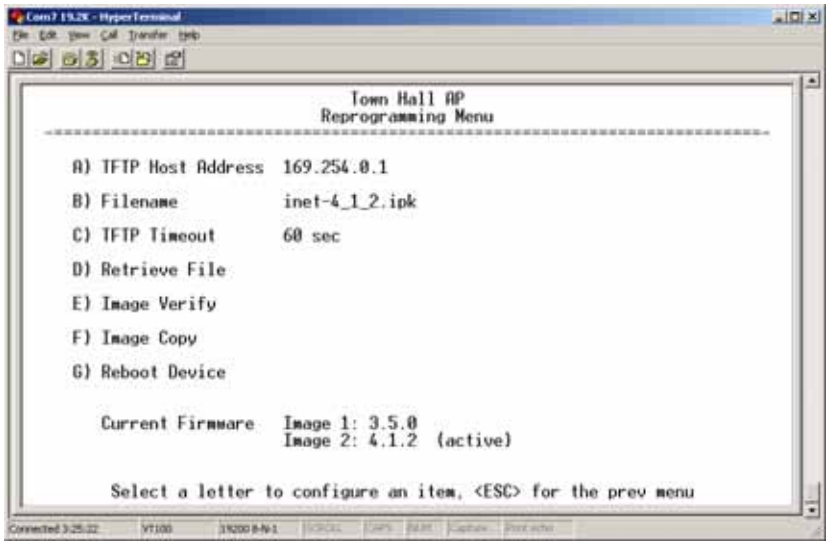

Town Hall AP
Reprogramming Menu
A) TFTP Host Address 169.254.0.1
B) Filename inet-4_1_2.ipk
C) TFTP Timeout 60 sec
D) Retrieve File
E) Image Verify
F) Image Copy
G) Reboot Device
Current Firmware Image 1: 3.5.0
Image 2: 4.1.2 (active)
Select a letter to configure an item, <ESC> for the prev menu

Figure 3-52. Reprogramming Menu
(Shown with "Image Copy" Selected)

- **TFTP Host Address**—IP address of the host computer from which to get the file. [**Any valid IP address**] This same IP address is used in other screens/functions (reprogramming, logging, etc.). Changing it here also changes it for other screens/functions.
- **Filename**—Name of file to be received by the TFTP server. [**Any 40-character alphanumeric string**] Verify that this corresponds to the TFTP directory location. May require sub-directory, for example: **\firmware\inet\inet-4_4_0.ipk.**
- **TFTP Timeout**—Time in seconds the TFTP server will wait for a packet ACK (acknowledgment) from the *transceiver* before suspending the file transfer. [**2 to 60 seconds; 10**]
- **Retrieve File**—Initiate the file transfer from the file from TFTP server. Placed into inactive firmware position in the *transceiver*'s non-volatile memory [**Y, N**]
- **Image Verify**—Initiate the verification of the integrity of firmware file held in unit.
- **Image Copy**—Initiate the copying of the active firmware into the inactive image.
- **Reboot Device**—Initiate rebooting the *transceiver*. This will interrupt data traffic through this unit, and the network if performed on an Access Point. Intended to be used to toggle between firmware images.

NOTE: See *"Upgrading the Firmware"* on Page 93 for details on setting up the TFTP server.

Upgrading the Firmware

From time-to-time MDS offers upgrades to the transceiver firmware. One version of the firmware provides core software resources for all transceiver models. Loading new firmware into the unit will not alter any privileges provided by Authorization Keys and does *not* require the transceiver be taken off-line until you want to operate the unit from the newly installed firmware image.

You must use the embedded Management System for all firmware activities, including uploading from a TFTP server.

File transfers can be initiated through any of the three Management System gateways:

- **Terminal-Emulator**—Use a terminal emulator program on your PC, such as HyperTerminal, connected directly to the transceiver's COM1 port via a serial cable.
- **Telnet**—Text-based access to the Management System through a network connection.
- **Web Browser**—Connect to the transceiver using a Web browser on a local PC connected directly to the radio's LAN port or associated network.

Firmware images are provided free-of-charge on the MDS Web site at:
www.microwavedata.com/service/technical/support

Installing New Firmware by TFTP

To install firmware by TFTP, you will need:

- A PC with a TFTP server running.
- The IP address of the PC running the TFTP server.

If you do not know your computer's address on a Windows PC, you can use the **RUN** function from the **Start** menu and enter **winipcfg** or **ipconfig** to determine your local PC's IP address. The IP address of the radio can be found under the Management Systems' **Configuration** menu.
(*See "Network Configuration Menu"* on Page 40.)

A TFTP server can be found on the MDS Web site at:
www.microwavedata.com/service/technical/support/downloads.asp

There are several alternatives to connecting the transceiver for firmware upgrade. Figure 3-53 and Figure 3-54 show two variations. It is essential all of the equipment be on the same subnet.

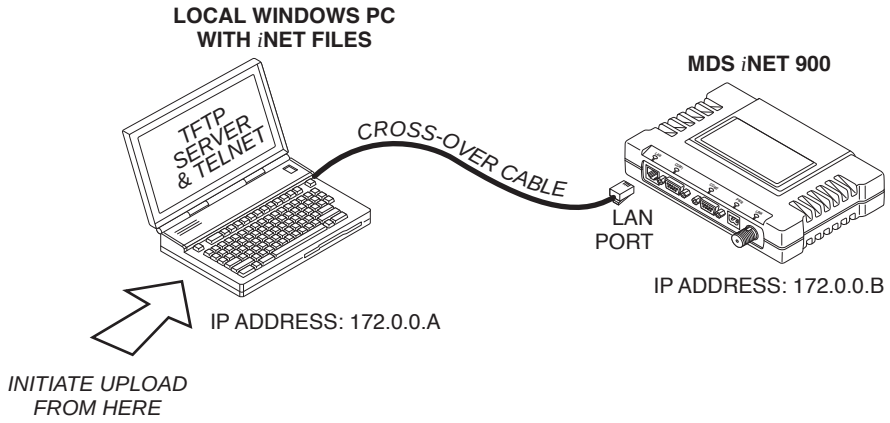


Figure 3-53. Firmware Upgrade Setup—Option 1
(TFTP Server and Firmware File on Same CPU)

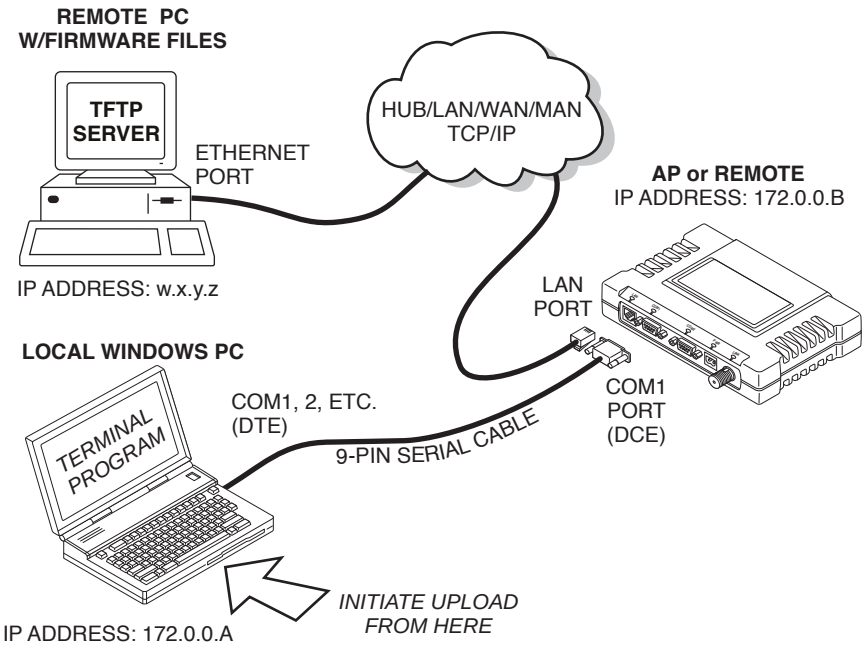


Figure 3-54. Firmware Upgrade Setup—Option 2
(TFTP Server and Firmware File on Remote Server)

NOTE: The LAN and COM1 ports share a common data channel when loading firmware over-the-air. Transferring the radio firmware image file (≈ 3 Mb), may take several minutes depending on traffic between the TFTP server and the transceiver.

Regardless of your connection to the transceiver, loading firmware/configuration files into the unit's flash-RAM is much slower than loading software onto a PC hard drive or RAM.

Upgrade Procedure

To load a new firmware file (**filename.ipk**) into the transceiver, use the following procedure:

1. Launch a TFTP server on a PC connected either directly or via a LAN to the Ethernet port (LAN) of the radio. Point the server towards the directory containing the firmware image file.

2. Connect to the Management System by whichever means is convenient: Browser or Telnet via the LAN, or Terminal emulator via the COM1 port.

3. Go to the MS Reprogramming Menu.
(**Main Menu>>Maintenance Menu>>Reprogramming Menu**)

4. Fill in the information for the:

   - **TFTP Host Address**—IP Address of server (host computer) running TFTP server.
   - **Retrieve File**—Name of file (**filename.ipk)** to be pulled from the TFTP server holding the firmware file.

5. Pull the firmware file through the TFTP server into the transceiver.
(**Main Menu>>Maintenance Menu>>Reprogramming Menu>>Retrieve File**)

   Status messages on the transfer are posted on the Management System screen.

NOTE: The new firmware image file that replaces the "Inactive Image" file will be automatically verified.

6. Reboot the transceiver.
Main Menu>>Maintenance Menu>>Reprogramming Menu>>Reboot Device

7. Test the transceiver for normal operation.

End of Procedure

Error Messages During File Transfers

It is possible to encounter errors during a file transfer. In most cases errors can be quickly corrected by referring to Table 3-6.

Table 3-6. Common Errors During TFTP Transfer

Error Message	Likely Cause/Corrective Action
Invalid File Type	Indicates that the file is not a valid firmware file. Locate proper file and re-load.
File not found	Invalid or non-existent filename on TFTP server
Invalid file path	Invalid or non-existent file path to TFTP server
Timeout	TFTP transfer time expired. Increase the timeout value.
Flash Error	Flash memory error. Contact factory for assistance.
Bad CRC	Cyclic Redundancy Check reporting a corrupted file. Attempt to re-load, or use a different file.
Version String Mismatch	Invalid file detected. Attempt to re-load, or use a different file.
Sending LCP Requests	The PPP server is querying for any clients that may need to connect.
Port not Enabled	The serial port is disabled.

3.9.2 Configuration Scripts Menu

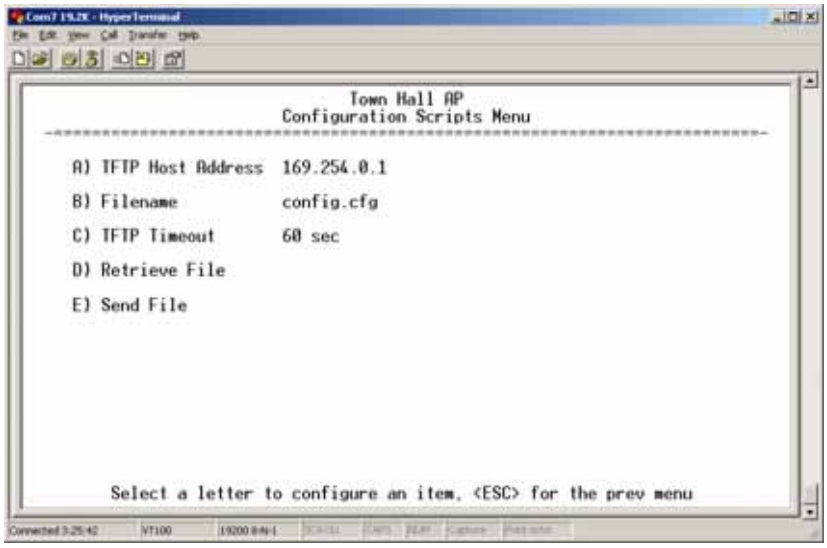

Town Hall AP
Configuration Scripts Menu
A) TFTP Host Address 169.254.0.1
B) Filename config.cfg
C) TFTP Timeout 60 sec
D) Retrieve File
E) Send File
Select a letter to configure an item, <ESC> for the prev menu

Figure 3-55. Configuration Files Menu

- **TFTP Host Address**—IP address of the computer on which the TFTP server resides. [**Any valid IP address**]
- **Filename**—Name of file containing this unit's configuration profile that will be transferred to the TFTP server. The configuration information will be in a plain-text ASCII format. [**Any 40-character alphanumeric string**] May require sub-directory, for example: **config\inet-config.txt**. (See *"Using Configuration Scripts"* on Page 98)

  NOTE: The filename field is used in identifying the desired incoming file and as the name of file being exported to the TFTP server. Before exporting the unit's configuration, you may want to name it something that reflect the unit's services or identification.
- **TFTP Timeout**—Time in seconds the TFTP server will wait for a packet ACK (acknowledgment) from the *transceiver* before suspending the file transfer. [**10 to 120 seconds; 10**]
- **Retrieve File**—Initiate the file transfer of the configuration file from TFTP server into the transceiver.
- **Send File**—Initiate the file transfer from the transceiver's current configuration file to TFTP server.

NOTE: See *Upgrading the Firmware* on Page 93 for details on setting up the TFTP server.

A Brief Description of Configuration Files

If you plan to have more than a few radios in your network, use the configuration file feature to configure similar units from a common set of parameters. There are over 50 user-controllable settings that can be used to optimize the network and saved into a Configuration File. However,

only four essential parameters need to be reviewed and altered to use the file with another transceiver.

A Configuration File (data file) will make it easy to apply your unique settings to any radio(s) you wish. Configuration files will also provide you with a tool to restore parameters to a "known good" set, in the event that a parameter is improperly set and performance is affected. (See *"Using Configuration Scripts"* on Page 98 for detailed instructions and a sample configuration file.)

Using Configuration Scripts

Configuration Scripts can be created and downloaded from the transceiver that contain a wealth of information on the unit. This file can serve many purposes, not the least of which is to keep a permanent "snapshot" of the unit's configuration at a point in time. These files can also be used to view the setup of a unit without needing to connect to it. Examining archival files can be a useful source of information during troubleshooting.

In the next few sections you will learn about the contents of the file and, how to use it as a template for configuring multiple transceivers with the same profile. Ultimately, standardized files can be uploaded into the transceiver to speed up the installation process.

Configuration Files can also be uploaded into a transceiver to restore the settings of a unit using a previously-saved configuration of the unit. This is particularly convenient after finishing a test using some experimental settings.

Sample of an Exported Configuration File

The following is a sample of a typical configuration file as produced by a transceiver containing over 150 parameters; many of which are user editable. The presentation has been slightly altered to allow notes to appear below associated parameter lines. Some of the values used in the calibration of the unit's built-in test equipment have been deleted to reduce space. This presentation is offered as a guide to the type of information contained in the file. See *"Editing Configuration Files"* on Page 104 for further information.

NOTE: The parameter names and the data values from the Exported Configuration File are shown in bolded text. Any description will be found below in an indented paragraph. Descriptions for parameters that are functionally identical to both COM1 & COM2 are not repeated.

Beginning of Configuration File

; MDS iNET

; Created 00-03-2002 6:59:41

IP Address: 192.168.1.1

The IPv4 address of this unit. This field is unnecessary if DHCP is enabled.

NOTE: Changing the IP value via the network will cause a loss of communication with other devices unaware of the new address.

IP Netmask: 255.255.255.0

The IPv4 local subnet mask. This field is unnecessary if DHCP is enabled.

IP Gateway: 0.0.0.0

The IPv4 address of the network gateway device, typically a router. This field is unnecessary if DHCP is enabled.

Ethernet Address: 00:06:3D:00:00:5D

The physical Ethernet MAC (Media Access Controller) address of the device. This value is set by the factory and cannot be changed.

Wireless Address: 00:06:3D:00:00:5C

The physical wireless MAC (Media Access Controller) address of the device. This value is set by the factory and cannot be changed.

Model Number: 900

The model number of this unit. This value is set by the factory and cannot be changed.

Serial Number: 1026295

The serial number of this unit. This value is set by the factory and cannot be changed.

Unit Name: Library Admin Office

A name for this unit. It appears at the top of every menu screen.

Owner: Hilltop College IT

The name of the owner of this unit.

Contact: IT Dept. X232

The contact person regarding this unit.

Description: Link to Campus Server

A brief general description of this unit.

Location: Hollister Bldg. RM450

The location of this unit.

Com1 Port Config: 8N1

Configuration of character size, type of parity, and number of stop bits to be used.

Com2 Port Config: 8N1

Configuration of character size, type of parity, and number of stop bits to be used

Max Remotes Allowed: 50

The maximum number of remotes allowed to connect to this Access Point.

Device Mode: Access Point

Configures the unit to act as a Remote or an Access Point. The Access Point option is not allowed unless the unit is specifically ordered as such, or an Authorization Key has been purchased to allow it.

Dwell Time: 32.8

The amount of time the unit spends at any given frequency in its hopping pattern. This field is only changeable by an Access Point. Remotes read the Masters value upon association.

Hop Pattern: 1

RSSH Calibration: 235

RSSL Calibration: 190

Freq Calibration: 8402

Network Name: West Campus Net

The name of the network this unit belongs to. The unit will only communicate with devices having identical *Network Names*.

Date Format: Generic

Specifies the format of the date.

- Generic = dd Mmm yyyy
- European = dd-mm-yyyy
- US = mm-dd-yyyy

Console Baud: 19200

The baud rate of the serial menu console. Default value is 19200 bps.

Company Name: MDS

Version Name: 06-1234567

Product Name: iNET

Beacon Period: Normal

The amount of time in milliseconds between beacon transmissions by the AP.

Data Rate: 512 kbps

The selected over-the-air data rate. A lower data rate generally allows more distance between the unit and its Access Point.

RF Output Power Setpoint: 30

The desired amount of RF output power, measured in dBm.

Power Cal Table DAC1: 98

21 additional values follow; do not alter

Active Boot Image: 0

Tx Coefficient1: 0

31 additional values follow; do not alter

Rx Coefficient1: 0

14 additional values follow; do not alter

Skipped Hop Zone1: Active

Skipped Hop Zone2: Skip

Skipped Hop Zone3: Active

Skipped Hop Zone4: Active

Skipped Hop Zone5: Active

Skipped Hop Zone6: Active

Skipped Hop Zone7: Active

Skipped Hop Zone8: Active

Skipped Hop Zone9: Active

Skipped Hop Zone10: Active

Firmware TFTP Host IP: 63.249.227.105

Address of the TFTP Host from which firmware images are downloaded

Firmware TFTP Filename: inet-4_4_0.ipk

Eventlog TFTP Host IP: 192.168.1.3

Address of TFTP Host to which to send the event log

Eventlog TFTP Filename:

Config Script TFTP Host IP: 192.168.1.33

Address of TFTP Host to which to send the event log

Config Script TFTP Filename: inet_config.txt

Fragmentation Threshold: 1600

Maximum packet size allowed before fragmentation occurs

RTS Threshold: 500

Number of bytes for the RTS/CTS handshake boundary

RSSI Threshold: 0

RSSI value at that the connection is deemed “degraded”

SNR Threshold: 0

SNR value at that the connection is deemed “degraded”

SNMP Read Community: public

Community string for read access using SNMPv1

SNMP Write Community: private

Community string for write access using SNMPv1

SNMP Trap Community: public

Community string sent with traps using SNMPv1

SNMP Trap Manager #1: 0.0.0.0

IP Address of a SNMP manager to which traps will be sent

SNMP Trap Manager #2: 0.0.0.0

SNMP Trap Manager #3: 0.0.0.0

SNMP Trap Manager #4: 0.0.0.0

SNMP Trap Manager #5: 0.0.0.0

Auth trap enable: disabled

Setting to enable SNMP authentication traps

Trap Version: v1 Traps

Selects which SNMP trap format

Package 1 Version: 1.1.0

Indicates the version of firmware in Image 1

Package 2 Version: 1.1.0

TFTP Timeout: 20

Com1 Serial Data Enable: disabled

Setting to enable COM1 data mode

Com1 Serial Data Mode: UDP

IP Protocol for COM1 data mode

Com1 Serial Data Baud Rate: 9600

Baud rate for COM1 data mode

Com1 Serial Data Tx IP Address: 0.0.0.0

COM1 data will be sent to this IP address

Com1 Serial Data Tx IP Port: 0

COM1 data will be sent to this IP port

Com1 Serial Data Rx IP Port: 0

COM1 data will be received on this IP port

Com2 Serial Data Enable: enabled

Com2 Serial Data Mode: UDP

Com2 Serial Data Baud Rate: 9600

Com2 Serial Data Tx IP Address: 169.254.10.2

Com2 Serial Data Tx IP Port: 0

Com2 Serial Data Rx IP Port: 0

Com1 Serial Data Rx IP Address: 0.0.0.0

COM1 data will be received on this IP address

Com2 Serial Data Rx IP Address: 169.254.0.2

Com2 Serial Data Flow Control: disabled

Enables hardware flow control (RTS/CTS) in COM2 data mode

SNTP Server IP: 0.0.0.0

The IPv4 address of NTP/SNTP Time Server

Com1 Serial Data Seamless Mode: enabled

Setting to enable seamless mode for COM1 data mode

Com2 Serial Data Seamless Mode: enabled

Com1 Serial Data Delimiter Chars: 4

Minimum number of characters which will be considered a gap in seamless mode for COM1

Com2 Serial Data Delimiter Chars: 4

Com1 Serial Data Buffer Size: 20

Number of output characters which will be buffered in seamless mode for COM1

Com2 Serial Data Buffer Size: 20

RF Frequency Hopping Format: USA/CANADA

(Read Only) The frequency-hopping rules the radio is configured to operate under

SNMP Enable: disabled

Enable/Disable SNMP Agent

Hop Protocol: 1

Frequency hopping protocol version

DHCP Server Enable: disabled

Enable/Disable DHCP Server Daemon

DHCP Netmask: 255.255.255.0

The IP Address to be used as the DHCP Netmask

DHCP Start Address: 192.168.0.11

The IP Address to be used as the starting address

DHCP End Address: 192.168.0.22

The IP Address to be used as the ending address

Approved Remotes List Enable: disabled

Setting to enable the Approved Remotes List

Encryption Enable: disabled

Setting to enable over-the-air data encryption

HTTP Enable: enabled

Setting to enable the HTTP interface

Telnet Enable: enabled

Setting to enable the Telnet interface

HTTP MD5 Authentication: disabled

Setting to enable MD5 Digest Authentication

Automatic Key Rotation: disabled

Setting to enable Automatic Key Rotation

Approved APs List Enable: disabled

Setting to enable the Approved Access Points List

Watch-Link-Status Flag @ AP: disabled

A flag that controls whether the Remotes care about the AP's Ethernet Link Status

Network Name Hash Enable: disabled

A flag that controls whether MD5 hashing is applied to the network name

End of Configuration File

Editing Configuration Files

Once a Remote unit's operation is fine-tuned, use the *Configuration Scripts Menu* on Page 97 to save a copy of the configuration in a PC. Once the file is saved in the PC it can be used as a source to generate modified copies adjusted to match other devices. The configuration files can be modified using a text editor or an automated process. (Not provided by MDS).

We recommend that you review and update the following parameters for each individual unit. Other parameters may also be changed.

Table 3-7. Common User-Alterable Parameters

Field	Comment	Range
IP Address	Unique for each individual radio	Any legal IP address
IP Gateway	May change for different groups or locations	Any legal IP address
Unit Name	Should reflect a specific device. This information will appear in Management System headings	Any 20-character alphanumeric string
Location	Used only as reference for network administration	Any 40-character alphanumeric string
System Mode	The application of the parameter in this field is dependent on the authorized options stored in the unit's permanent memory. The mode must be compatible with any previously installed Authorization Keys.	"Access Point" "Dual Remote" "Serial Remote" "Ethernet Remote" NOTE: These are case-sensitive.
Network Name	Used to identify different groups or locations	Any 15-character alphanumeric string

Each resulting file should be saved with a different name. We recommend using directories and file names that reflect the location of the unit to facilitate its identification.

Editing Rules

- You may include only parameters you want to change.
- Change only the parameter values.
- Capitalization counts in some field parameters. (Example: System Mode)
- Comment Fields
    a. Edit, or delete anything on each line to the right of the comment delineator, the semicolon (;).
    b. Comments can be of any length, but must be on the same line as the parameter, or on a new line that begins with a semicolon character.
    c. Comments after parameters in files exported from a transceiver do not need to be present in your customized files.

3.9.3 Authorization Keys Menu

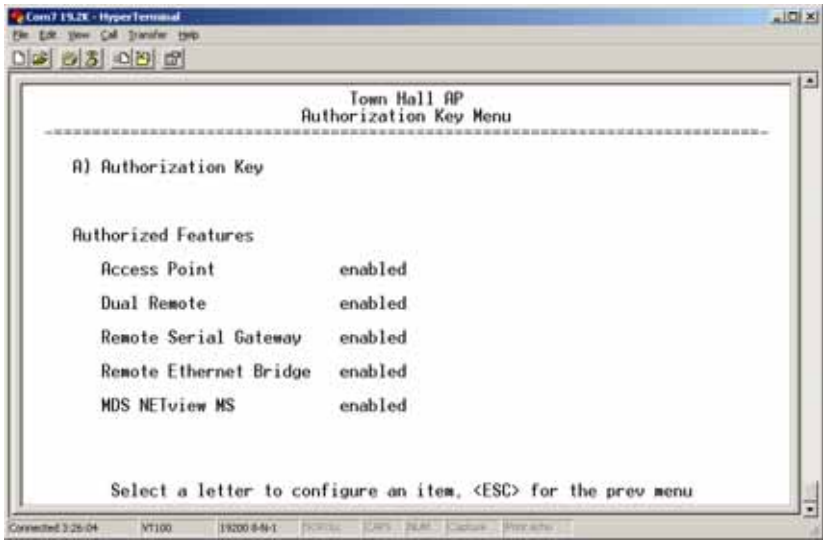

Town Hall AP
Authorization Key Menu
A) Authorization Key
Authorized Features
Access Point enabled
Dual Remote enabled
Remote Serial Gateway enabled
Remote Ethernet Bridge enabled
MDS NETview MS enabled
Select a letter to configure an item, <ESC> for the prev menu

Figure 3-56. Authorization Key Menu

- **Authorization Key**—Initiate the entering of an Authorization Key into the transceiver's non-volatile memory.
- **Authorized Features**—List of authorized features.

  In addition to the four configurations fields, is the **MDS NETview MS** access control. *NETview MS* is designed to help users monitor system performance, configure network elements, detect faults and correct problems in the convenience of an office setting or at any other point in the network.

3.9.4 Auto-Upgrade/Remote-Reboot Menu

NOTE: This menu is only available when MDS NETview MS key is enabled.

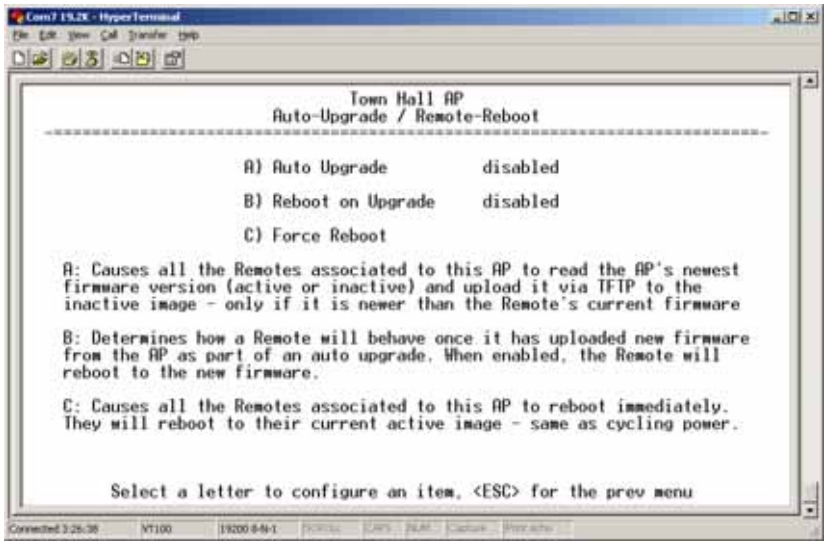

Town Hall AP
Auto-Upgrade / Remote-Reboot
A) Auto Upgrade disabled
B) Reboot on Upgrade disabled
C) Force Reboot
A: Causes all the Remotes associated to this AP to read the AP's newest firmware version (active or inactive) and upload it via TFTP to the inactive image - only if it is newer than the Remote's current firmware
B: Determines how a Remote will behave once it has uploaded new firmware from the AP as part of an auto upgrade. When enabled, the Remote will reboot to the new firmware.
C: Causes all the Remotes associated to this AP to reboot immediately. They will reboot to their current active image - same as cycling power.
Select a letter to configure an item, <ESC> for the prev menu

Figure 3-57. Auto-Upgrade / Remote Reboot Menu

- **Auto Upgrade**—Causes all of the Remotes associated to this AP to read the AP's newest firmware version (active or inactive) and upload it via TFTP to the inactive image, but only if it is newer than the Remote's current firmware.
- **Reboot on Upgrade**—Determines how a Remote will behave once it has uploaded new firmware from the AP as part of an auto-upgrade. When enabled, the Remote will reboot to the new firmware.
- **Force Reboot**—Causes all of the Remotes associated to this AP to reboot immediately. They will reboot to their current active image—the same as if the power were re-cycled.

NOTE: To use the Auto Upgrade/Reboot feature, both the AP and Remotes must already be running version 4.4.0 or newer firmware.

Exception: If the AP has already been upgraded to version 4.4.0 and the Remote is still at 3.5.0 or older, you can upgrade the Remote by using the AP as a file server. This method allows for only one remote to be upgraded at a time. Instructions for this method are given below.

Firmware Upgrade (with AP Acting as a File Server)

An AP running firmware version 4.4.0 (or newer) may be used as a file server to upgrade Remotes running older firmware (3.5.0 or earlier). Follow the steps below to perform the upgrade:

1. At the Reprogramming Menu (Page 92), Enter the AP's IP Address in the TFTP Server field.

2. Enter **upgrade_from_ap.ipk** in the Filename field.

NOTE: The filename is case sensitive.

3. Perform the firmware download.

3.9.5 Radio Test Menu

This area provides several useful tools for installers and maintainers. You can manually key the radio transmitter to make measurements of antenna performance. (See *"Antenna Aiming"* on Page 125 for details.)

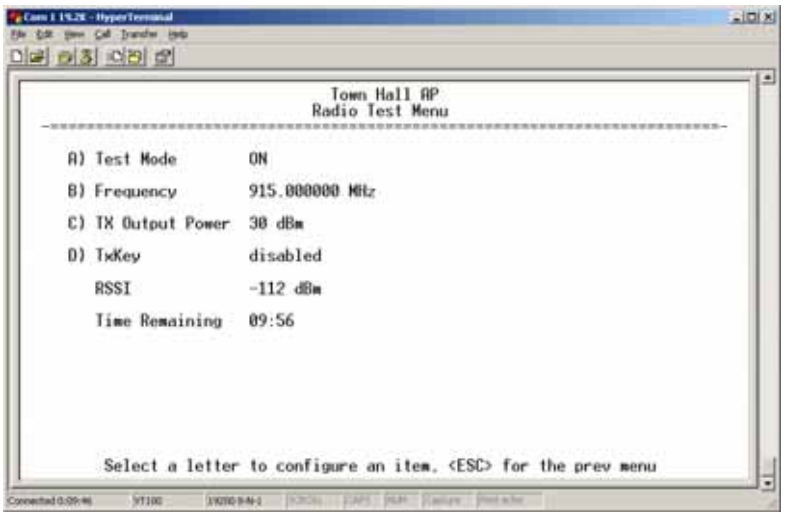

Town Hall AP
Radio Test Menu
A) Test Mode ON
B) Frequency 915.000000 MHz
C) TX Output Power 30 dBm
D) TxKey disabled
RSSI -112 dBm
Time Remaining 09:56
Select a letter to configure an item, <ESC> for the prev menu

Figure 3-58. Radio Test Menu
Shown with Test Mode set to ON

NOTE : Use of the Test Mode will disrupt traffic through the radio. If the unit is an Access Point, it will disrupt traffic through the *entire* network.

Test Mode function is automatically limited to 10 minutes and *should only be used for brief measurement of transmit power*. It may also be manually reset to continue with the testing or turned off.

- **Test Mode**—Controls access to the transceiver's suite of tools. [**ON, OFF; OFF**]
- **Frequency**—Set radio operating frequency during the testing period to a single frequency. [**915.0000 MHz**]
- **TX Output Power**—Temporarily overrides the power level setting in the Radio Configuration Menu. [**20**]

- **TxKey**—Manually key the radio transmitter for power measurements. [**Enable, Disable; Disable**]
- **RSSI**—Incoming received signal strength on frequency entered in the frequency parameter on this screen (–dBm).

  This RSSI measurement is updated more frequently than the RSSI by Zone display of the Performance Information menu.

3.9.6 Ping Utility Menu

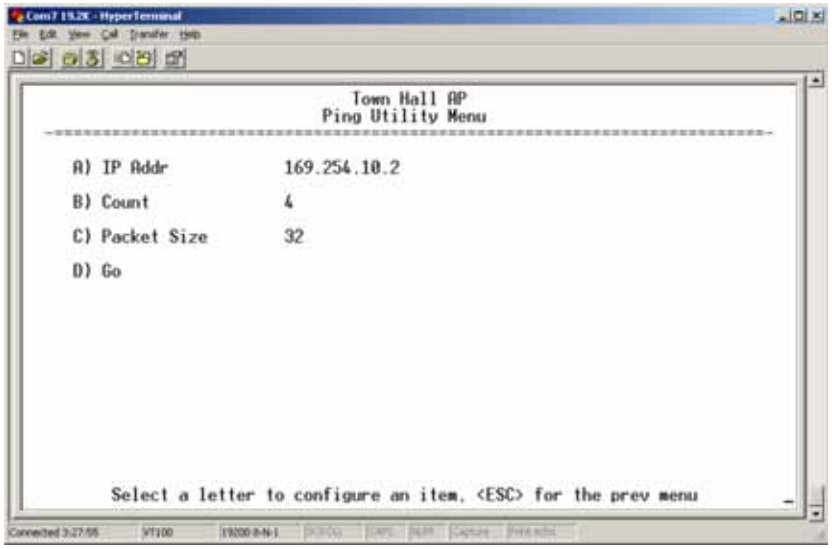

Town Hall AP
Ping Utility Menu
A) IP Addr 169.254.10.2
B) Count 4
C) Packet Size 32
D) Go
Select a letter to configure an item, <ESC> for the prev menu

Figure 3-59. Ping Utility Menu

- **IP Addr**—Address to send a PING. [**Any valid IP address**]
- **Count**—Number of PING packets to be sent.
- **Packet Size**—Size of each PING data packet (bytes).
- **Go**—Send PING packets to address shown on screen.

  Screen will be replaced with detailed report of PING activity. Press any key after viewing the results to return to this menu.

3.9.7 Reset to Factory Defaults

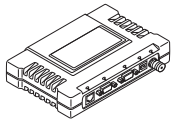
To reset all transceiver parameters back to the factory defaults, you must enter a special code (authorization key) provided by the factory in place of the user name.

This procedure is useful when several parameters have been modified, and there is no track of changes. The transceiver returns to a known state, where it may be easier to determine the correct settings.

3.9.8 Resetting the Password

The user has the ability to return the *i*NET password to the default value of **admin** by entering a specific MDS-supplied authorization key at the login prompt. This event causes all radio parameters to return to the fac-

tory default settings. Because of this, if the person requesting the password-reset authorization key is not the true owner, any custom configuration settings from the true owner are erased. This prevents the new person from recovering the network settings of the true owner.



4 TROUBLESHOOTING & RADIO MEASUREMENTS

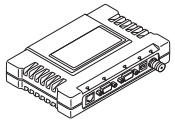
Contents

4.1 TROUBLESHOOTING 113

4.1.1 Interpreting the Front Panel LEDs 113
4.1.2 Troubleshooting Using the Embedded Management System .. 114
4.1.3 Using Logged Operation Events 118
4.1.4 Alarm Conditions 118
4.1.5 Correcting Alarm Conditions 120
4.1.6 Logged Events 121

4.2 RADIO (RF) MEASUREMENTS 123

4.2.1 Antenna System SWR and Transmitter Power Output 124
4.2.2 Antenna Aiming 125



4.1 TROUBLESHOOTING

Successful troubleshooting of a wireless system is not difficult, but requires a logical approach. It is best to begin troubleshooting at the Access Point unit, as the rest of the system depends on the Access Point for synchronization data. If the Access Point has problems, the operation of the entire wireless network will be affected.

When communication problems are found, it is good practice to begin by checking the simple things. Applying basic troubleshooting techniques in a logical progression can identify many problems.

Multiple Communication Layers

It is important to remember the operation of the network is built upon a radio communications link. On top of that are two data levels— wireless MAC, and the data layer. It is essential that the wireless aspect of the Access Point and the Remotes units to be associated are operating properly before data-layer traffic will function.

Unit Configuration

There are over 50 user-configurable parameters in the Management System. Do not overlook the possibility that human error may be the cause of the problem. With so many possible parameters to look at and change, a parameter may be incorrectly set, and then what was changed is forgotten.

To help avoid these problems, we recommend creating an archive of the transceiver's profile when your installation is complete in a Configuration File. This file can be reloaded into the transceiver to restore the unit to the factory defaults or your unique profile. For details on creating and archiving Configuration Files, see *"Using Configuration Scripts"* on Page 98.

Factory Assistance

If problems cannot be resolved using the guidance provided here, review the MDS web site's technical support area for recent software/firmware updates, general troubleshooting help, and service information. Additional help is available through our Technical Support Department. (See "TECHNICAL ASSISTANCE" on the inside of the rear cover.)

4.1.1 Interpreting the Front Panel LEDs

An important set of troubleshooting tools are the LED status indicators on the front panel of case. You should check them first whenever a problem is suspected. Table 2-2 on Page 23 describes the function of each status LED. Table 4-1 below provides suggestions for resolving

common system difficulties using the LEDs, and Table 4-2 provides other simple techniques.

Table 4-1. Troubleshooting Using LEDs—Symptom-Based

Symptom	Problem/Recommended System Checks
PWR LED does not turn on	a. Voltage too low—Check for the proper supply voltage at the power connector. (10–30 Vdc) b. Indefinite Problem—Cycle the power and wait (≈ 30 seconds) for the unit to reboot. Then, recheck for normal operation.
LINK LED does not turn on	a. Network Name of Remote not identical to desired Access Point—Verify that the system has a unique Network Name. b. Not yet associated with an Access Point with the same Network Name. Check the "Status" of the unit's process of associating with the Access Point. Use the Management System. c. Poor Antenna System—Check the antenna, feedline and connectors. Reflected power should be less than 10% of the forward power reading (SWR 2:1 or lower).
PWR LED is blinking	a. Blinking indicates an alarm condition exists. b. View Current Alarms and Event Log and correct the problem if possible. (See *"Using Logged Operation Events"* on Page 118) c. Blinking will continue until the source of the alarm is corrected, for example, a valid IP address is entered, etc.
LAN LED does not turn on	a. Verify the Ethernet cable is connect at both ends. b. Verify that the appropriate type of Ethernet cable is used: straight-through, or crossover.
LAN LED lights, but turns off after some time	Verify traffic in LAN. Typically, the radio should not be placed in high traffic enterprise LANs, as the it will not be able to pass this level of traffic. If needed, use routers to filter traffic.

4.1.2 Troubleshooting Using the Embedded Management System

If you have reviewed and tried the things mentioned in Table 4-1 and still have not resolved the problem, there are some additional tools and techniques that can be used. The embedded Management System is a good source of information that may be used remotely to provide preliminary diagnostic information, or may even provide a path to correcting the problem.

Table 4-2. Basic Troubleshooting Using the Management System

Symptom	Problem/Recommended System Checks
Remote does not associate; stays in HOPSYNC	a. Verify the AP has sufficiently large number in the "Max Remotes" parameter of the Network Configuration Menu. b. Verify the correct MAC address is listed in the "Approved Remotes List" or "Approved Access Points List" of the Security Configuration menu.
Serial data is slow with UDP multicast traffic	Change Beacon Period to FAST. (Radio Configuration Menu)
Cannot access the MS through COM1	a. Connect to unit via Telnet or Web browser b. Disable the serial mode for COM1 (Serial Gateway Configuration>>Com1 Serial Data Port>>Status>>Disabled) or, if you know the unit's data configuration: a. Connect to COM 1 via a terminal set to VT100 and the port's data baud rate. b. Type **+++** c. Change the terminal's baud rate to match the transceiver's Console Baud Rate. d. Type **+++**
Display on terminal/Telnet screen garbled	Verify the terminal/terminal emulator or Telnet application is set to VT100
Cannot pass IP data to WAN.	a. Verify your IP settings. b. Use the PING command to test communication with the transceivers in the local radio system. c. If successful with local PING, attempt to PING an IP unit attached to a transceiver. d. If successful with the LAN PINGs, try connecting to a known unit in the WAN.
Wireless Retries too high.	Possible Radio Frequency Interference— a. If omnidirectional antennas are used, consider changing to directional antennas. This will often limit interference to and from other stations. b. Try skipping some zones where persistent interference is known or suspected. c. The installation of a filter in the antenna feedline may be necessary. Consult the factory for further assistance.
Password forgotten.	a. Connect to the transceiver using a terminal through the COM1 Port. b. Obtain a password-resetting Authorization Key from your factory representative. c. Enter the Authorization Key at the login prompt as a password.
Packet Repeat Mode troubles (extra characters in data, data not delivered)	Verify that all radios in the network have their Packet Redundancy Mode set to the same selection (Single Packet vs. Packet Repeat Mode).

The following is a summary of how several screens in the Management System can be used as diagnostic tools. For information on how to connect to the Management System See *"STEP 3—CONNECT PC TO THE TRANSCEIVER"* on Page 20.

Starting Information Screen

*(*See *Starting Information Screen* on Page 36*)*

The Management System's "homepage" provides some valuable bits of data. One of the most important is the "Device Status" field. This item will tell you if the unit is showing signs of life.

If the *Device Status* field says "associated," then look in the network areas beginning with network data statistics. If it displays some other message, such as *Scanning*, *Hop Sync* or *Alarmed*, you will need to determine why it is in this state.

The Scanning state indicates a Remote unit is looking for an Access Point beacon signal to lock onto. It should move to the Hop Sync and finally to the Associated state within less than a minute. If this Remote unit is not providing reliable service, look at the *Event Logs* for signs of lost association with the Access Point or low signal alarms. Table 4-3 provides a description of the Device Status messages.

Table 4-3. Device Status[1]

Scanning	The unit is looking for an Access Point beacon signal. If this is a Remote radio, *Associated* means that this unit is associated with an Access Point
Hop Sync	The unit has found a valid beacon signal for its network and has changed its frequency hopping pattern to match that of the AP.
Associated	This unit has successfully synchronized and is "associated" with an Access Point. This is the normal operating state.
Alarmed	The unit is has detected one or more alarms that have not been cleared.

1. Available in the *Startup Information Screen* or the *Wireless Status Screen* at the Remotes.

If the Remote is in an "Alarmed" state, the unit may still be operational and associated. Look for the association state in the *Wireless Network Status* screen to determine if the unit is associated. If it is, then look at the *Error Log* for possible clues.

If the unit is in an "Alarmed" state and not able to associate with an Access Point unit, then there may be problem with the wireless network layer. Call in a radio technician to deal with wireless issues. Refer the technician to the *RADIO (RF) MEASUREMENTS* on Page 123 for information on antenna system checks.

Packet Statistics Menu

(See Packet Statistics Menu on Page 81)

This screen provides detailed information on data exchanges between the unit being viewed and the network through the wireless and the Ethernet (data) layers. These include:

Wireless Packet Statistics

- Packets received
- Packets sent
- Bytes received
- Bytes sent
- Packets dropped
- Receive errors
- Retries
- Retry errors

Ethernet Packet Statistics

- Packets received
- Packets sent
- Bytes received
- Bytes sent
- Lost carrier detected
- Packets dropped
- Receive errors
- Retries
- Retry errors

The most significant fields are the *Packets Dropped*, *Retries*, *Retry Errors*, *Receive Errors* and *Lost Carrier Detected*. If the data values are more than 10% of their sent and received counterparts, or the *Lost Carrier Detected* value is greater than a few dozen, there may be trouble with radio-frequency interference or a radio link of marginal strength. Review the *RSSI by Zone Screen's* values (Page 77) for zones that are more than 2 dB (decibels) below the average level, and for signal level values that are likely to provide marginal service. For example, an average level is less than –85 dBm during normal conditions with a data rate of 256 kbps.

If the RSSI levels in each zone are within a few dB of each other, but less than –85 dBm, then a check should be made of the aiming of the antenna system and for a satisfactory SWR. Refer to *RADIO (RF) MEASUREMENTS* on Page 123 for information on antenna system checks.

NOTE: For a data rate of 512 kbps, the average signal level should be –77 dBm or stronger with no interference.

Serial Port Statistics Menu

(See Serial Data Statistics Menu on Page 87)

This screen provides top-level information on data exchanges between the unit's serial ports and the network through the wireless and the Ethernet (data) layers. These include:

- Bytes In On Port *xxx*
- Bytes Out On Port *xxx*
- Bytes In On Socket *xxx*
- Bytes Out On Socket *xxx*

You can use this screen as a indicator of port activity at the data and IP levels.

Diagnostic Tools

(See MAINTENANCE on Page 91)

The radio's Maintenance menu contains two tools that are especially useful to network technicians—the Radio Test Menu and the Ping Utility. The Radio Test selection allows for testing RF operation, while the Ping Utility can be used to verify reachability to pieces of equipment connected to the radio network. This includes transceivers and user-supplied Ethernet devices.

4.1.3 Using Logged Operation Events

(See Event Log Menu on Page 78)

The transceiver's microprocessor monitors many operational parameters and logs them as various classes of "events". If the event is one that affects performance, it is an "alarmed". There are also normal or routine events such as those marking the rebooting of the system, implementation of parameter changes and external access to the Management System. Informational events are stored in temporary (RAM) memory that will be lost in the absence of primary power, and Alarms will be stored in permanent memory (Flash memory) until cleared by user request. Table 3-5 summarizes these classifications.

Table 4-4. Event Classifications

Level	Description/Impact	Storage
Informational	Normal operating activities	Flash Memory
Minor	Does not affect unit operation	RAM
Major	Degraded unit performance but still capable of operation	RAM
Critical	Prevents the unit from operating	RAM

These various events are stored in the transceiver's "Event Log" and can be a valuable aid in troubleshooting unit problems or detecting attempts at breaching network security.

4.1.4 Alarm Conditions

(See View Current Alarms on Page 80)

Most events, classified as "critical" will make the PWR LED blink, and will inhibit normal operation of the transceiver. The LED blinks until the corrective action is completed.

Table 4-5. Alarm Conditions (Alphabetical Order)

Alarm Condition Reported	Event Log Entry	SNMP Trap
EVENT_50_LIMIT	Crossed 50% of Eth Port Rate Limit	rateLimit50(20)
EVENT_75_LIMIT	Crossed 75% of Eth Port Rate Limit	rateLimit75(21)
EVENT_100_LIMIT	Crossed 100% of Eth Port Rate Limit	rateLimit100(22)
EVENT_ADC	ADC output Railed	adcInput(3)
EVENT_AP_NN_CHANGED	Network Name changed at the AP	apNetNameChanged(74)
EVENT_BRIDGE	Network Interface /Error	networkInterface(17)
EVENT_CHILE_CHAN_CNT	Mismatch in Chilean Channel count at AP/REM	chileChanCnt(71)
EVENT_CHILE_NO_CHAN	Using Chilean hopping but no channels selected	chileNoChan(23)
EVENT_COMPRESS	Compression setting changed	compressionChanged(76)
EVENT_ENDPOINT	Endpoint Added/Removed (AP only)	eventEndpoint(67)
EVENT_ETH_LINK_AP*	AP Ethernet Link Disconnected	apEthLinkLost(19)
EVENT_FLASH_TEST	Flash Test Failed	-
EVENT_FPGA	FPGA communication Failed	fpgaCommunication(2)
EVENT_FREQ_CAL	Frequency Not Calibrated	frequencyCal(7)
EVENT_INIT_ERR	Initialization Error	initializationError(18)
EVENT_IPADDR*	IP Address Invalid	ipAddressNotSet(4)
EVENT_IP_CONN(OK)		ipConnectivityOK(75)
EVENT_IPMASK*	IP Mask Invalid	ipNetmaskNotSet(5)
EVENT_LAN_PORT		lanPortStatus(78)
EVENT_MAC	MAC communication Failed	macCommunication(1)
EVENT_MACADDR	MAC Address Invalid	noMacAddress(6)
EVENT_NETNAME*	Netname Invalid	invalidNetname(12)
EVENT_PLL_LOCK	PLL Not locked	pllLock(10)
EVENT_POWER_CAL	Power Calibrated/Not Calibrated	powerCal(8)
EVENT_POWER_HIGH	RF Power Control Saturated High	rfPowerHigh(13)
EVENT_POWER_LOW	RF Power Control Saturated Low	rfPowerLow(14)

Table 4-5. Alarm Conditions (Alphabetical Order) *(Continued)*

Alarm Condition Reported	Event Log Entry	SNMP Trap
EVENT_REMOTE	Remote Added/ Removed (AP only)	eventRemote(66)
EVENT_REPETITIVE	The previous event is occurring repetitively	
EVENT_ROUTE_ADD	Manual entry added to Routing table	routeAdded(68)
EVENT_ROUTE_DEL	Manual entry deleted from Routing table	routeDeleted(69)
EVENT_RSSI*	RSSI Exceeds threshold	rssi(11)
EVENT_RSSI_CAL	RSSI Not Calibrated	rssiCal(9)
EVENT_SDB_ERR	Internal Remote/Endpoint database error (AP only)	sdbError(80)
EVENT_SINREM_SWITCH	Eth/Serial mode switch in a Single Remote	sinRemSwitch(70)
EVENT_SYSTEM_ERROR*	System Error Cleared; Please Reboot	systemError(16)
EVENT_TFTP_CONN	TFTP connectivity achieved	tftpConnection(73)
EVENT_TFTP_ERR	Attempted TFTP connection failed	tftpConnFailed(79)

* Condition may be corrected by user and alarm cleared.

4.1.5 Correcting Alarm Conditions

(See View Event Log on Page 81)

Table 4-6 provides insight on the causes of events that inhibit the unit from operating, and possible corrective actions. The Event Description column appears on the **Event Log** screen.

Table 4-6. Correcting Alarm Conditions—Alphabetical Order

Event Log Entry	Generating Condition	Clearing Condition or Action
ADC Failure	The ADC always reads the same value (either high or low limit)	Contact factory Technical Services for assistance
AP Ethernet Link	Monitor will check state of Ethernet link and set alarm if it finds the link down	Ethernet link is re-established
Bridge Down	When the Bridge fails to be initialized	Contact factory Technical Services for assistance
Flash Test Failed	Internal check indicates corruption of Flash memory	Contact factory Technical Services for assistance
FPGA Failure	Communication lost to the FPGA	Contact factory Technical Services for assistance

Table 4-6. Correcting Alarm Conditions—Alphabetical Order

Event Log Entry	Generating Condition	Clearing Condition or Action
General System Error	Internal checks suggest unit is not functioning properly	Reboot the transceiver
Initialization Error	Unit fails to complete boot cycle	Contact factory Technical Services for assistance
Invalid IP Address	The IP address is either 0.0.0.0 or 127.0.0.1	Program IP address to something other than 0.0.0.0 or 127.0.0.1
MAC Failure	The monitor task reads the LinkStatus from the MAC every second. If the MAC does not reply 10 consecutive times (regardless of what the result is) the CPU assumes the transceiver has lost communication to the MAC.	Contact factory Technical Services for assistance
Network Interface Error	Unit does not recognize the LAN interface	Contact factory Technical Services for assistance
Network Name Not Programmed	Network name is “Not Programmed”	Change Network Name to something other than “Not Programmed”
PLL Out-of-Lock	The FPGA reports a synthesizer out-of-lock condition when monitored by the CPU.	Contact factory Technical Services for assistance.
Power Control Railed High	Power control can no longer compensate and reaches the high rail	Contact factory Technical Services for assistance
Power Control Railed Low	Power control can no longer compensate and reaches the low rail	Contact factory Technical Services for assistance
RSSI Exceeds Threshold	The running-average RSSI level is weaker (more negative) than the user-defined value.	Check aiming of the directional antenna used at the Remote; or raise the threshold level to a stronger (less-negative) value.

4.1.6 Logged Events

(See View Event Log on Page 81)

The following events allow the transceiver to continue operation and do not make the PWR LED blink. Each is reported through an SNMP trap.

The left hand column, “Event Log Entry” is what will be shown in the Event Log.

Table 4-7. Non-Critical Events—Alphabetical Order

Event Log Entry	Severity	Description
Association Attempt Success/Failed	MAJOR	Self explanatory
Association Lost - AP Hop Parameter Changed	MINOR	Self explanatory
Association Lost - AP's Ethernet Link Down	MAJOR	Self explanatory
Association Lost - Local IP Address Changed	MAJOR	Self explanatory
Association Lost - Local Network Name Changed	MAJOR	Self explanatory
Association Lost/Established	MAJOR	Self explanatory
Auth Demo Mode Expired -- Rebooted Radio/Enabled	MAJOR	Self explanatory
Auth Key Entered - Key Valid/Key Invalid	MAJOR	Self explanatory
Bit Error Rate Below threshold/Above threshold	INFORM	Self explanatory
Console Access Locked for 5 Min	MAJOR	Self explanatory
Console User Logged Out/Logged In	MAJOR	Self explanatory
Country/SkipZone Mismatch	INFORM	Self explanatory
Current AP No Longer Approved	MAJOR	May occur during the Scanning process at a remote. Indicates that the received beacon came from an AP which is not in the “Approved AP” list. This may be caused by some remotes hearing multiple AP's. This event is expected behavior.
Decryption Error/Decryption OK		A decryption error is logged when an encryption phrase mismatch has occurred. A mismatch is declared after five consecutive errors over a 40-second window. When the error has cleared, **DECRYPT OK** will appear.
Desired AP IP Addr Mismatch	INFORM	Self explanatory
ETH Rate		Indicates heavy bursts of traffic on the unit's Ethernet port (LAN). This is expected behavior, resulting from the network configuration.
Ethernet Port Enabled/Disabled	INFORM	Self explanatory
Expected Sync Lost/Established	INFORM	Self explanatory
Hop Sync Lost/Established	INFORM	Self explanatory

Table 4-7. Non-Critical Events—Alphabetical Order *(Continued)*

Event Log Entry	Severity	Description
Hop Table Generated/Generation Failed	INFORM	Self explanatory
HTTP Access Locked for 5 Min	MAJOR	Self explanatory
HTTP User Logged Out/Logged In	MAJOR	httpLogin(49)
Log Cleared	INFORM	Self explanatory
MAC Param Changed		Caused by remotes running in auto data rate mode. Every time the link conditions cause a data rate change, the remote's MAC changes to the new rate and forwards a signal to the AP. This indicates link quality is changing and causing the data rate to adjust accordingly.
Max Beacon Wait Time Exceeded	MAJOR	Self explanatory
Received Beacon - AP is Blacklisted	INFORM	Self explanatory
Received Beacon - Netname Does Not Match	INFORM	Self explanatory
Received Beacon - Valid/Errored	INFORM	Self explanatory
Rem Ethernet Link Connected/Disconnected	MAJOR	Self explanatory
Reprogramming Complete	INFORM	Self explanatory
Reprogramming Failed	MAJOR	Self explanatory
Reprogramming Started	INFORM	Self explanatory
Scanning Started	INFORM	Self explanatory
SNR Within threshold/Below threshold	INFORM	Self explanatory
System Bootup (power on)	INFORM	Self explanatory
Telnet Access Locked for 5 Min	MAJOR	Self explanatory
Telnet User Logged Out/Logged In	MAJOR	Self explanatory
User Selected Reboot	MAJOR	Self explanatory

4.2 RADIO (RF) MEASUREMENTS

There are several measurements that are a good practice to perform during the initial installation. The will confirm proper operation of the unit and if they are recorded, serve as a benchmark in troubleshooting should difficulties appear in the future. These measurements are:

- Transmitter Power Output
- Antenna System SWR (Standing-Wave Ratio)

- Antenna Direction Optimization

These procedures may interrupt traffic through an established network and should only be performed by a skilled radio-technician in cooperation with the network manager.

4.2.1 Antenna System SWR and Transmitter Power Output

Introduction

A proper impedance match between the transceiver and the antenna system is important. It ensures the maximum signal transfer between the radio and antenna. The impedance match can be checked indirectly by measuring the SWR (standing-wave ratio) of the antenna system. If the results are normal, record them for comparison for use during future routine preventative maintenance. Abnormal readings indicate a possible trouble with the antenna or the transmission line that will need to be corrected.

The SWR of the antenna system should be checked before the radio is put into regular service. For accurate readings, a wattmeter suited to 1000 MHz measurements is required. One unit meeting this criteria is the Bird Model 43™ directional wattmeter with a 5J element installed.

The reflected power should be less than 10% of the forward power (≈2:1 SWR). Higher readings usually indicate problems with the antenna, feedline or coaxial connectors.

If the reflected power is more than 10%, check the feedline, antenna and its connectors for damage.

Record the current transmitter power output level, and then set it to 30 dBm for the duration of the test to provide an adequate signal level for the directional wattmeter.

Procedure

1. Place a directional wattmeter between the ANTENNA connector and the antennas system.

2. Place the transceiver into the Radio Test Mode using the menu sequence below:
   (Main Menu>>Maintenance Menu>>Radio Test>>Test Mode>>Y>>ON)

NOTE: The Test Mode has a 10-minute timer, after which it will return the radio to normal operation. The Radio Test Mode can be terminated manually by selecting **OFF** on the menu or temporarily disconnecting the radio's DC power.

---

3. Set the transmit power to 30 dBm. (This setting does not affect the output level during normal operation—only during Test Mode.)
   (Main Menu>>Maintenance Menu>>Radio Test>>Test Mode>>Tx Power Output)

4. Key the transmitter.
   (Main Menu>>Maintenance Menu>>Radio Test>>Test Mode>>TxKey>>Enable)

   Use the PC's spacebar to key and unkey the transmitter ON and OFF. (Enable/Disable)

5. Measure the forward and reflected power into the antenna system and calculate the SWR and power output level. The output should agree with the programmed value.

   (Main Menu>>Radio Configuration>>RF Power Output)

6. Turn off Radio Test Mode at the Access Point and Remote.
   (Main Menu>>Maintenance Menu>>Radio Test>>Test Mode>>Disable)

End of procedure

4.2.2 Antenna Aiming

Introduction

The radio network integrity depends, in a large part, on stable radio signal levels being received at each end of a data link. In general, signal levels stronger than –77 dBm (–80 dBm for *i*NET II) provides the basis for reliable communication that includes a 15 dB fade margin. As the distance between the Access Point and Remotes increases, the influence of terrain, foliage and man-made obstructions become more influential and the use of directional antennas at Remote locations becomes necessary. Directional antennas usually require some fine-tuning of their bearing to optimize the received signal strength. The transceiver has a built-in received signal strength indicator (RSSI) that can be used to tell you when the antenna is in a position that provides the optimum received signal.

RSSI measurements and Wireless Packet Statistics are based on multiple samples over a period of several seconds. The average of these measurements will be displayed by the Management System.

The measurement and antenna alignment process will usually take 10 or more minutes at each radio unit.

The path to the Management System menu item is shown in bold text below each step of the procedure.

Procedure

1. Verify the Remote transceiver is associated with an Access Point unit by observing the condition of the LINK LED (**LINK LED = On or Blinking**). This indicates that you have an adequate signal level for the measurements and it is safe to proceed.

2. View and record the *Wireless Packets Dropped* and *Received Error* rates.
   (Main Menu>>Performance Information>>Packet Statistics>>Wireless Packet Statistics)

   This information will be used later.

3. Clear the *Wireless Packets Statistics* history.

   (Main Menu>>Performance Information>>Packet Statistics>>Wireless Packet Statistics>>Clear Wireless Stats)\

4. Read the RSSI level at the Remote.
   (Main Menu>>Performance Information>>RSSI by Zone)

5. Optimize RSSI (less negative is better) by slowly adjusting the direction of the antenna.

   Watch the RSSI indication for several seconds after making each adjustment so that the RSSI accurately reflects any change in the link signal strength.

6. View the *Wireless Packets Dropped* and *Received Error* rates at the point of maximum RSSI level. They should be the same or lower than the previous reading.

   (Main Menu>>Performance Information>>Packet Statistics>>Wireless Packet Statistics)

   If the RSSI peak results in an increase in the *Wireless Packets Dropped* and *Received Error*, the antenna may be aimed at an undesired signal source. Try a different antenna orientation.

End of procedure

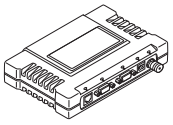
5 PLANNING A RADIO NETWORK

Contents

5.1 INSTALLATION PLANNING 129

5.1.1 General Requirements 129
5.1.2 Site Selection 131
5.1.3 Terrain and Signal Strength 131
5.1.4 Antenna & Feedline Selection 132
5.1.5 How Much Output Power Can be Used? 135
5.1.6 Conducting a Site Survey 135
5.1.7 A Word About Radio Interference 136

5.2 dBm-WATTS-VOLTS CONVERSION CHART 139



5.1 INSTALLATION PLANNING

This section provides tips for selecting an appropriate site, choosing an antenna system, and reducing the chance of harmful interference.

5.1.1 General Requirements

There are three main requirements for installing a transceiver—adequate and stable primary power, a good antenna system, and the correct interface between the transceiver and the data device. Figure 5-1 shows a typical Remote Gateway installation.

NOTE: The *i*NET 900 network port supports 10BaseT connections, but does not support 100BaseT connections. This should not present a problem because most hubs/switches auto-switch between 10BaseT and 100BaseT connections. Confirm that your hub/switch is capable of auto-switching data rates.

To prevent Ethernet traffic from degrading *i*NET 900 performance, place the *i*NET in a segment, or behind routers.

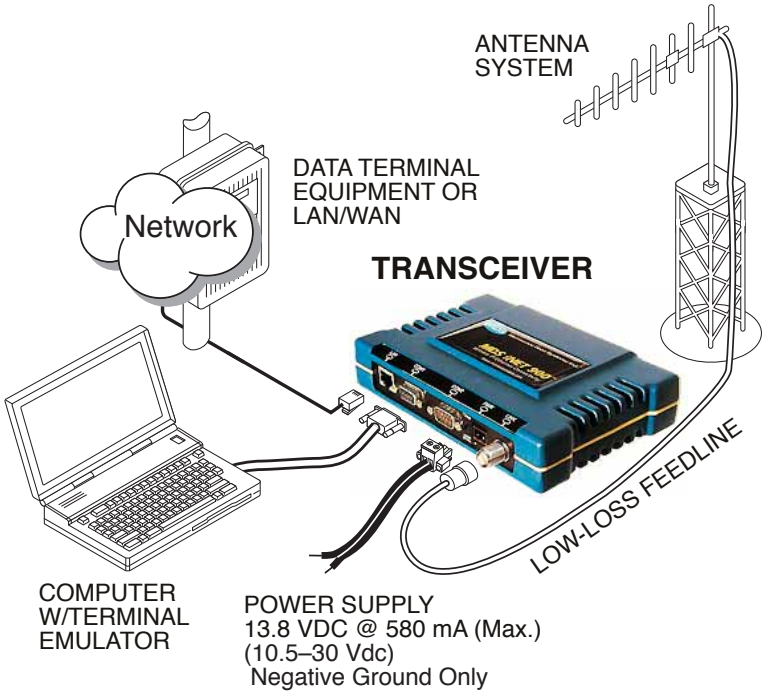


Figure 5-1. Typical Installation with a Tower-Mounted Antenna
(Connect user data equipment to any compatible LAN or COM Port)

Unit Dimensions

Figure 5-2 shows the dimensions of the transceiver case and its mounting holes, and Figure 5-3 on Page 131, the dimensions for mounting with factory-supplied brackets. If possible, choose a mounting

location that provides easy access to the connectors on the end of the radio and an unobstructed view of the LED status indicators.

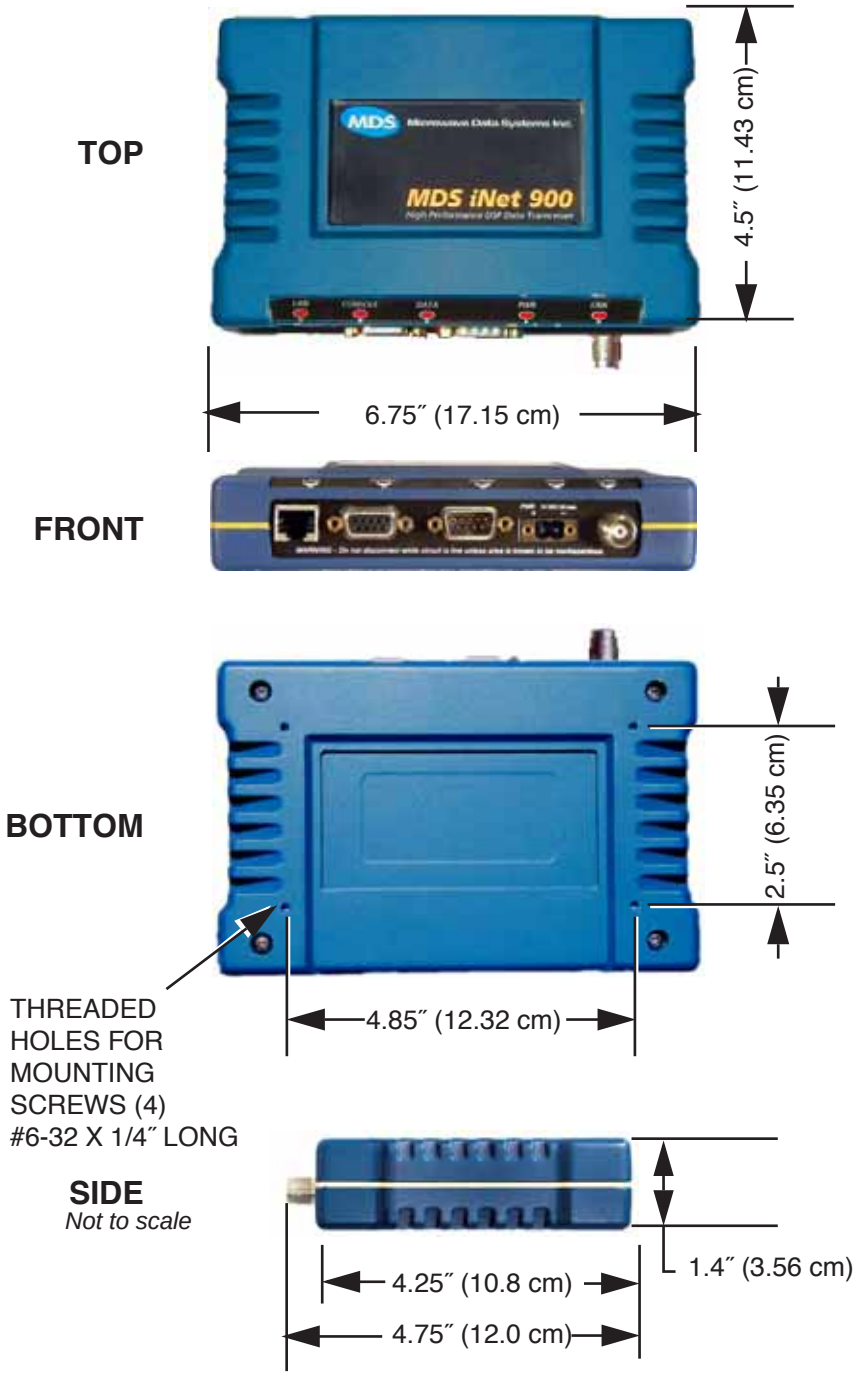


Figure 5-2. Transceiver Dimensions

Figure 5-3. Mounting Bracket Dimensions

5.1.2 Site Selection

Suitable sites should provide:

- Protection from direct weather exposure
- A source of adequate and stable primary power
- Suitable entrances for antenna, interface or other required cabling
- Antenna location that provides as unobstructed a transmission path as possible in the direction of the associated station(s)

These requirements can be quickly determined in most cases. A possible exception is the last item—verifying that an unobstructed transmission path exists. Radio signals travel primarily by line-of-sight, and obstructions between the sending and receiving stations will affect system performance. If you are not familiar with the effects of terrain and other obstructions on radio transmission, the discussion below will provide helpful background.

5.1.3 Terrain and Signal Strength

While the license-free 900 MHz band offers many advantages for data transmission services, signal propagation is affected by attenuation from obstructions such as terrain, foliage or buildings in the transmission path.

A line-of-sight transmission path between the central transceiver and its associated remote site(s) is highly desirable and provides the most reliable communications link.

Much depends on the minimum signal strength that can be tolerated in a given system. Although the exact figure will differ from one system to another, a Received Signal Strength Indication (RSSI) of –77 dBm (–80 dBm for *i*NET II) or stronger will provide acceptable performance in many systems. While the equipment will work at lower-strength signals, signals stronger than – 77 dBm provide a “fade margin” of 15 dB to

account for variations in signal strength that may occur from time-to-time. RSSI can be measured with a terminal connected to the COM1 Port or with a HTTP browser to the LAN (Ethernet) connector. (See *"Antenna Aiming"* on Page 125 for details.)

5.1.4 Antenna & Feedline Selection

NOTE: The transceiver is a Professional Installation radio system and must be installed by trained professional installers, or factory trained technicians.

This text that follows is designed to aid the professional installer in the proper methods of maintaining compliance with FCC Part 15 limits and the +36 dBm or 4 watts peak E.I.R.P limit.

Antennas

The equipment can be used with a number of antennas. The exact style used depends on the physical size and layout of a system. Contact your factory representative for specific recommendations on antenna types and hardware sources.

In general, an omnidirectional antenna (Figure 5-4) is used at the Access Point station site. This provides equal coverage to all of the Remote Gateway sites.

NOTE: Antenna polarization is important. If the wrong polarization is used, a signal reduction of 20 dB or more will result. Most systems using a gain-type omnidirectional antenna at the Access Point station employ vertical polarization of the signal; therefore, the remote antenna(s) must also be vertically polarized (elements oriented perpendicular to the horizon).

When required, horizontally polarized omnidirectional antennas are also available. Contact your factory representative for details.

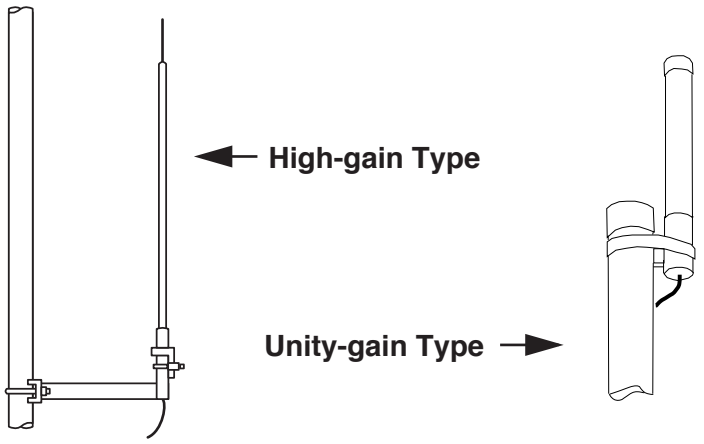


Figure 5-4. Typical Omnidirectional Antennas

At Remote Gateway sites and units in point-to-point LANs, a directional Yagi (Figure 5-5) antenna is generally recommended to minimize interference to and from other users. Antennas are available from a number of manufacturers.

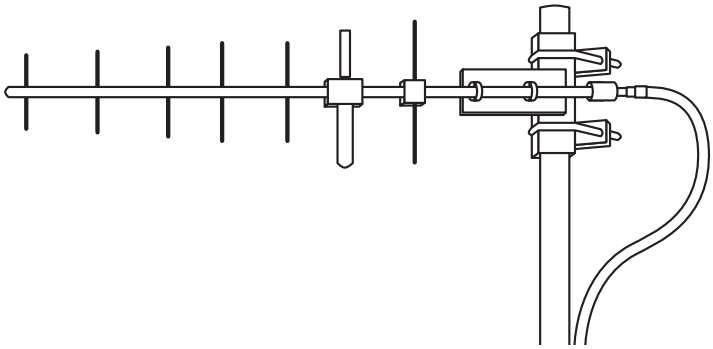


Figure 5-5. Typical Yagi Antenna (mounted to mast)

Feedlines

The choice of feedline used with the antenna should be carefully considered. Poor-quality coaxial cables should be avoided, as they will degrade system performance for both transmission and reception. The cable should be kept as short as possible to minimize signal loss.

For cable runs of less than 20 feet (6 meters), or for short range transmission, an inexpensive type such as Type RG-8A/U may be acceptable. Otherwise, we recommend using a low-loss cable type suited for 900 MHz, such as Heliax®.

Table 5-1 lists several types of popular feedlines and indicates the signal losses (in dB) that result when using various lengths of cable at

900 MHz. The choice of cable will depend on the required length, cost considerations, and the amount of signal loss that can be tolerated.

Table 5-1. Length vs. Loss in Coaxial Cables at 900 MHz

Cable Type	10 Feet (3.05 m)	50 Feet (15.24 m)	100 Feet (30.48 m)	500 Feet (152.4 m)
RG-214	.76 dB	3.8 dB	7.6 dB	Unacceptable Loss
LMR-400	0.39 dB	1.95 dB	3.90 dB	Unacceptable Loss
1/2 inch HELIAX	0.23 dB	1.15 dB	2.29 dB	11.45 dB
7/8 inch HELIAX	0.13 dB	0.64 dB	1.28 dB	6.40 dB
1-1/4 inch HELIAX	0.10 dB	0.48 dB	0.95 dB	4.75 dB
1-5/8 inch HELIAX	0.08 dB	0.40 dB	0.80 dB	4.00 dB

The tables below outline the minimum lengths of RG-214 coaxial cable that must be used with common MDS omnidirectional antennas in order to maintain compliance with FCC maximum limit of +36 dBi. If other coaxial cable is used, the appropriate changes in loss figures must be made.

NOTE: The authority to operate the transceiver in the USA may be void if antennas other than those approved by the FCC are used. Contact your MDS representative for additional antenna information.

Table 5-2. Feedline Length vs. Antenna Gain*

(Required for Regulatory compliance)

Antenna Gain (dBd)	Antenna Gain (dBi)	Minimum Feedline Length (Loss in dB)	EIRP Level @ Min. Length	Maxrad Antenna Part No.
Unity (0 dB)	2.15 dBi	No minimum length	+32.15 dBm	Omni #MFB900
3 dBd	5.15 dBi	No minimum length	+35.15 dBm	Omni # MFB900
5 dBd	7.15 dBi	3.1 meters (1.2 dB)	+35.95 dBm	Omni # MFB900
6 dBd	8.15 dBi	9.1 meters (2.2 dB)	+35.95 dBm	Yagi # BMOY8903
10 dBd	12.15 dBi	24.7 meters (6.15 dB)	+35.25 dBm	Yagi # Z941

*Refer to Table 5-3 for allowable power settings of the transceiver for each antenna type.

NOTE: There is no minimum feedline length required when a 6 dBi gain or less antenna is used, as the EIRP will never exceed 36 dBm which is the maximum allowed, per FCC rules. The transceiver's RF output power may only be adjusted by the manufacturer or its sub-contracted Professional Installer.

The MDS *i*NET II Transceiver is factory set to +29 dBm power output to maintain compliance with the FCC's Digital Transmission System (DTS) Part 15 rules. These rules limit power to a maximum of 8 dBm/3 kHz, thus the *i*NET II Transceiver is factory set to +29 dBm. When calculating maximum transceiver power output for *i*NET II installations, use +29 dBm if antenna gain is 6 dBi or less. See *How Much Output Power Can be Used?* on Page 135 for power control of higher gain antennas.

5.1.5 How Much Output Power Can be Used?

The transceiver is normally supplied from the factory set for a nominal +30 dBm (+29 dBm for *i*NET II) RF power output setting; this is the maximum transmitter output power allowed under FCC rules. The power must be *decreased* from this level if the antenna system gain exceeds 6 dBi. The allowable level is dependent on the antenna gain, feedline loss, and the transmitter output power setting.

NOTE: In some countries, the maximum allowable RF output may be limited to less than the figures referenced here. Be sure to check for and comply with the requirements for your area.

5.1.6 Conducting a Site Survey

If you are in doubt about the suitability of the radio sites in your system, it is best to evaluate them before a permanent installation is underway. This can be done with an on-the-air test (preferred method); or indirectly, using path-study software.

An on-the-air test is preferred because it allows you to see firsthand the factors involved at an installation site and to directly observe the quality of system operation. Even if a computer path study was conducted earlier, this test should be done to verify the predicted results.

The test can be performed by first installing a radio and antenna at the proposed Access Point (AP) station site (one-per-system). Then visit the Remote site(s) with another transceiver (programmed as a remote) and a hand-held antenna. (A PC with a network adapter can be connected to each radio in the network to simulate data during this test using the PING command.)

With the hand-held antenna positioned near the proposed mounting spot, a technician can check for synchronization with the Access Point

station (shown by a lit LINK LED on the front panel) and measure the reported RSSI value. (See *"Antenna Aiming"* on Page 125 for details.) If adequate signal strength cannot be obtained, it may be necessary to mount the station antennas higher, use higher gain antennas, select a different site or consider installing a repeater station. To prepare the equipment for an on-the-air test, follow the general installation procedures given in this guide and become familiar with the operating instructions found in the *CHAPTER-3 EMBEDDED MANAGEMENT SYSTEM* section Page 25.

5.1.7 A Word About Radio Interference

The transceiver shares the radio-frequency spectrum with other 900 MHz services and other Part 15 (unlicensed) devices in the USA. As such, near 100% error-free communications may not be achieved in a given location, and some level of interference should be expected. However, the radio's flexible design and hopping techniques should allow adequate performance as long as care is taken in choosing station location, configuration of radio parameters and software/protocol techniques.

In general, keep the following points in mind when setting up your communications network.

- Systems installed in rural areas are least likely to encounter interference; those in suburban and urban environments are more likely to be affected by other devices operating in the license-free frequency band and by adjacent licensed services.
- Use a directional antenna at remote sites whenever possible. Although these antennas may be more costly than omnidirectional types, they confine the transmission and reception pattern to a comparatively narrow lobe, that minimizes interference to (and from) stations located outside the pattern.
- If interference is suspected from a nearby licensed system (such as a paging transmitter), it may be helpful to use horizontal polarization of all antennas in the network. Because most other services use vertical polarization in this band, an additional 20 dB of attenuation to interference can be achieved by using horizontal polarization. Another approach is to use a bandpass filter to attenuate all signals outside the 900 MHz band.
- Multiple Access Point units can co-exist in proximity to each other with only very minor interference. Each network name has a different hop pattern. (See *"Protected Network Operation using Multiple Access Points"* on Page 12.) Additional isolation can be achieved by using separate directional antennas with as much vertical or horizontal separation as is practical.
- If constant interference is present in a particular frequency zone (collection of 8 RF channels), it may be necessary to "skip" that

zone from the radio's hopping pattern. The radio includes built-in software to help users identify and remove blocked frequency zones from its hopping pattern. See Page 56 for more information on Skip Zones.

- If interference problems persist even after skipping some zones, try reducing the length of data streams. Groups of short data streams have a better chance of getting through in the presence of interference than do long streams.
- The power output of all radios in a system should be set for the lowest level necessary for reliable communications. This lessens the chance of causing unnecessary interference to nearby systems.

If you are not familiar with these interference-control techniques, contact your factory representative for more information.

Calculating System Gain

To determine the maximum allowable power setting of the radio, perform the following steps:

1. Determine the antenna system gain by subtracting the feedline loss (in dB) from the antenna gain (in dBi). For example, if the antenna gain is 9.5 dBi, and the feedline loss is 1.5 dB, the antenna system gain would be 8 dB. (If the antenna system gain is 6 dB or less, no power adjustment is required.)

2. Subtract the antenna system gain from 36 dBm (the maximum allowable EIRP). The result indicates the maximum transmitter power (in dBm) allowed under the rules. In the example above, this is 28 dBm.

3. If the maximum transmitter power allowed is less than 30 dBm, set the power to the desired level using the Management System. (**Main Menu>>Radio Configuration>>RF Output Power Setpoint**)

For convenience, Table 5-3 lists several antenna system gains and shows the maximum allowable power setting of the radio. Note that a gain of 6 dB or less entitles you to operate the radio at full power output –30 dBm (28.7 dBm for *i*NET II).

Table 5-3. Antenna System Gain vs. Power Output Setting

Antenna System Gain (Antenna Gain in dBi* minus Feedline Loss in dB†)	Maximum Power Setting (PWR command) iNET Radio	Maximum Power Setting (PWR command) iNET II Radio	EIRP (in dBm)
Omni 6 (or less)	30	28	36
Omni 9	27	26	36
Yagi 12	24	23	36
Yagi 14	22	Not allowable	36
Yagi 16	20	Not allowable	36

* Most antenna manufacturers rate antenna gain in dBd in their literature. To convert to dBi, add 2.15 dB.

† Feedline loss varies by cable type and length. To determine the loss for common lengths of feedline, see Table 5-1 on Page 134.

For assistance in the conversion of dBm to Watts, please see *dBm-WATTS-VOLTS CONVERSION CHART* on Page 139.

5.2 dBm-WATTS-VOLTS CONVERSION CHART

Table 5-4 is provided as a convenience for determining the equivalent voltage or wattage of an RF power expressed in dBm.

Table 5-4. dBm-Watts-Volts conversion—for 50 ohm systems

dBm	V	Po
+53	100.0	200W
+50	70.7	100W
+49	64.0	80W
+48	58.0	64W
+47	50.0	50W
+46	44.5	40W
+45	40.0	32W
+44	32.5	25W
+43	32.0	20W
+42	28.0	16W
+41	26.2	12.5W
+40	22.5	10W
+39	20.0	8W
+38	18.0	6.4W
+37	16.0	5W
+36	14.1	4W
+35	12.5	3.2W
+34	11.5	2.5W
+33	10.0	2W
+32	9.0	1.6W
+31	8.0	1.25W
+30	7.10	1.0W
+29	6.40	800mW
+28	5.80	640mW
+27	5.00	500mW
+26	4.45	400mW
+25	4.00	320mW
+24	3.55	250mW
+23	3.20	200mW
+22	2.80	160mW
+21	2.52	125mW
+20	2.25	100mW
+19	2.00	80mW
+18	1.80	64mW
+17	1.60	50mW
+16	1.41	40mW
+15	1.25	32mW
+14	1.15	25mW
+13	1.00	20mW
+12	.90	16mW
+11	.80	12.5mW
+10	.71	10mW
+9	.64	8mW
+8	.58	6.4mW
+7	.500	5mW
+6	.445	4mW
+5	.400	3.2mW
+4	.355	2.5mW
+3	.320	2.0mW
+2	.280	1.6mW
+1	.252	1.25mW

dBm	V	Po
0	.225	1.0mW
-1	.200	.80mW
-2	.180	.64mW
-3	.160	.50mW
-4	.141	.40mW
-5	.125	.32mW
-6	.115	.25mW
-7	.100	.20mW
-8	.090	.16mW
-9	.080	.125mW
-10	.071	.10mW
-11	.064	
-12	.058	
-13	.050	
-14	.045	
-15	.040	
-16	.0355	

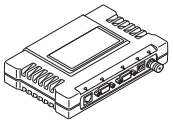
dBm	mV	Po
-17	31.5	
-18	28.5	
-19	25.1	
-20	22.5	.01mW
-21	20.0	
-22	17.9	
-23	15.9	
-24	14.1	
-25	12.8	
-26	11.5	
-27	10.0	
-28	8.9	
-29	8.0	
-30	7.1	.001mW
-31	6.25	
-32	5.8	
-33	5.0	
-34	4.5	
-35	4.0	
-36	3.5	
-37	3.2	
-38	2.85	
-39	2.5	
-40	2.25	.1μW
-41	2.0	
-42	1.8	
-43	1.6	
-44	1.4	
-45	1.25	
-46	1.18	
-47	1.00	
-48	0.90	

dBm	mV	Po
-49	0.80	
-50	0.71	.01μW
-51	0.64	
-52	0.57	
-53	0.50	
-54	0.45	
-55	0.40	
-56	0.351	
-57	0.32	
-58	0.286	
-59	0.251	
-60	0.225	.001μW
-61	0.200	
-62	0.180	
-63	0.160	
-64	0.141	

dBm	μV	Po
-65	128	
-66	115	
-67	100	
-68	90	
-69	80	
-70	71	.1nW
-71	65	
-72	58	
-73	50	
-74	45	
-75	40	
-76	35	
-77	32	
-78	29	
-79	25	
-80	22.5	.01nW
-81	20.0	
-82	18.0	
-83	16.0	
-84	11.1	
-85	12.9	
-86	11.5	
-87	10.0	
-88	9.0	
-89	8.0	
-90	7.1	.001nW
-91	6.1	
-92	5.75	
-93	5.0	
-94	4.5	
-95	4.0	
-96	3.51	
-97	3.2	

dBm	μV	Po
-98	2.9	
-99	2.51	
-100	2.25	.1pW
-101	2.0	
-102	1.8	
-103	1.6	
-104	1.41	
-105	1.27	
-106	1.18	

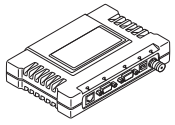
dBm	nV	Po
-107	1000	
-108	900	
-109	800	
-110	710	.01pW
-111	640	
-112	580	
-113	500	
-114	450	
-115	400	
-116	355	
-117	325	
-118	285	
-119	251	
-120	225	.001pW
-121	200	
-122	180	
-123	160	
-124	141	
-125	128	
-126	117	
-127	100	
-128	90	
-129	80	.1fW
-130	71	
-131	61	
-132	58	
-133	50	
-134	45	
-135	40	
-136	35	
-137	33	
-138	29	
-139	25	
-140	23	.01fW



6 TECHNICAL REFERENCE

Contents

6.1 DATA INTERFACE CONNECTORS 143
6.1.1 LAN Port 143
6.1.2 COM1 Port 144
6.1.3 COM2 Port 144
6.2 FUSE REPLACEMENT PROCEDURE 145
6.3 TECHNICAL SPECIFICATIONS 146
6.4 CHANNEL HOP TABLE 149
6.5 SNMP USAGE NOTES 151
6.5.1 Overview 151



6.1 DATA INTERFACE CONNECTORS

Three data interface connectors are provided on the face of the transceiver. The first, the LAN Port, is an RJ-45 connector. The other two use two DB-9 interface connectors that use the RS-232 (EIA-232) signaling standard. Note that the connector for COM1 Port is DCE (Female DB-9) and the COM2 Port is DTE (male DB-9).

CAUTION
RADIO FREQUENCY INTERFERENCE POTENTIAL

The transceiver meets U.S.A.'s FCC Part 15, Class A limits when used with shielded data cables.

6.1.1 LAN Port

The transceiver's LAN Port is used to connect the radio to an Ethernet network. The transceiver provides a data link to an Internet Protocol-based (IP) network via the Access Point station. Each radio in the network must have a unique IP address for the network to function properly.

- To connect a PC directly to the radio's LAN port, an RJ-45 to RJ-45 cross-over cable is required.
- To connect the radio to a Ethernet hub or bridge, use a straight-through cable.

The connector uses the standard Ethernet RJ-45 cables and wiring. For custom-made cables, use the pinout information below.

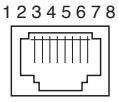


Figure 6-1. LAN Port (RJ-45) Pinout
(Viewed from the outside of the unit)

Table 6-1. LAN Port (IP/Ethernet)

Pin	Functions	Ref.
1	Transmit Data (TX)	High
2	Transmit Data (TX)	Low
3	Receive Data (RX)	High
4	Unused	
5	Unused	
6	Receive Data (RX)	Low
7	Unused	
8	Unused	

6.1.2 COM1 Port

To connect a PC to the transceiver's COM1 port use a DB-9M to DB-9F "straight-through" cable. These cables are available commercially, or may be constructed using the pinout information in Figure 6-2 and Table 6-2.

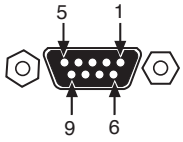


Figure 6-2. COM1 Port (DCE)
(Viewed from the outside of the unit.)

Table 6-2. COM1 Port Pinout, DB-9F/RS-232 Interface

Pin	Functions	DCE
1	Unused	
2	Receive Data (RXD)	<—[Out
3	Transmit Data (TXD)	—>[In
4	Unused	
5	Signal Ground (GND)	
6–9	Unused	

6.1.3 COM2 Port

To connect a PC to the transceiver's COM2 port use a DB-9F to DB-9M "straight-through" cable. These cables are available commercially, or may be constructed using the pinout information in Figure 6-2 and Table 6-2.

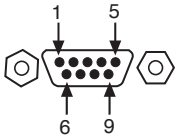


Figure 6-3. COM2 Port (DTE)
Viewed from the outside of the radio

Table 6-3. COM2 Port, DB-9M/EIA-232 Interface

Pin	Functions	DTE
1	Data Carrier Detect (DCD)	In]<—
2	Receive Data (RXD)	In]<—
3	Transmit Data (TXD)	Out]—>
4	Data Terminal Ready (DTR)	Out]—>
5	Signal Ground (GND)	

Table 6-3. COM2 Port, DB-9M/EIA-232 Interface

Pin	Functions	DTE
6	Data Set Ready (DSR)	In]<—
7	Request-to-Send (RTS)	Out]—>
8	Clear-to-Send (CTS)	In]<—
9	Unused	

6.2 FUSE REPLACEMENT PROCEDURE

An internal fuse protects the transceiver from over-current conditions or an internal component failure. It should not be replaced until you are certain you are in a safe (non-flammable) environment.

1. Disconnect the primary power source and all other connections to the unit.

2. Place the radio on its back and remove the four Phillips screws on the bottom cover.

3. Carefully separate the top and bottom covers. There is a flat ribbon cable between the top cover's LEDs and the unit motherboard. You do not need to disconnect the ribbon cable.

4. Locate the fuse and fuse holder between the COM1 port and the power connector. See Figure 6-4 for details.

5. Loosen the fuse from the holder using a very small screwdriver. Use a small pair of needle-nose pliers to pull the fuse straight up and remove it.

6. Using an Ohmmeter, or other continuity tester, verify the fuse is blown.

7. Install a new fuse by reversing the process.

   Littelfuse P/N: 0454002; 452 Series, 2 Amp SMF Slo-Blo
   MDS P/N: 29-1784A03

8. Install the covers and check the transceiver for proper operation.

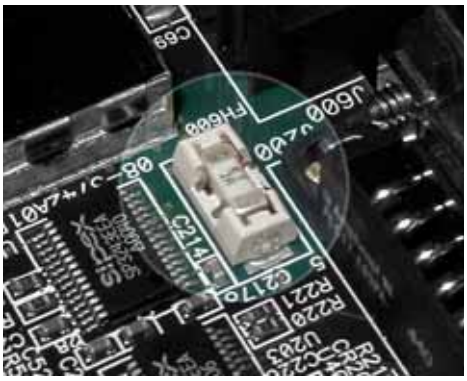


Figure 6-4. Internal Fuse and Holder Assembly Location

6.3 TECHNICAL SPECIFICATIONS

GENERAL

Temperature Range:	–30° C to +60° C (–22° F to 140° F)
Humidity:	95% at +40° C (104° F); non-condensing
Primary Power:	10–30 Vdc (13.8 Vdc Nominal)
External Power Supply Options:	110–120/210–220 Vac
Supply Current (typical):	(9 Watts Maximum @ 1 Watt RF Output)
Transmit:	8 watts (10.5-24 Vdc) 9 watts (24.5-30 Vdc)
Receive:	2.8 watts (10.5-24 Vdc) 3.5 watts (24.5-30 Vdc)
MTBF:	35 Years (Telcordia Method 1, Case 3)
Size (Excluding mtg. hardware):	1.4" x 6.75" x 4.5" (H x W x D) 3.56 x 17.15 x 11.43 cm
Mounting w/Optional Hardware:	• Flat surface mounting brackets
	• 19” rack (1U high)
Weight:	908 g / 2 lb
Case:	Cast Aluminum
Boot Time:	≈ 30 sec
Time Required to Associate with Access Point:	≈ 20 sec

APPROVALS/HOMOLOGATION

- FCC Part 15.247
  E5MDS-NH900
- Industry Canada RSS-210 and RSS-139
  CAN 3738A 12098
- UL/CSA Class 1, Div. 2; Groups A, B, C and D hazardous locations
- Contact factory for information on availability and governmental approvals in other countries

MANAGEMENT TOOLS

- HTTP (Embedded Web server)
- Text-based menu on COM1 serial port
- Telnet
- SNMP v1/v2/v3
- MDS NETview MS™

DATA CHARACTERISTICS

PORTS:

Ethernet:

Interface Connectors:	RJ-45 Standard
Data Rate:	10BaseT

Serial (2 Ports):

Signaling Standard:	EIA-232/V.24
Interface Connectors:	DB-9
Interface:	COM1: DCE / COM2: DTE
Data Rate:	1200–115,200 bps asynchronous
Data Latency:	< 10 ms typical
Byte Formats:	7 or 8-bit; even, odd, or no-parity; 1 or 2 stop bits

OPERATING MODES:

- Configurable as Access Point or Station LAN Adapter
- CSMA/CA Wireless Protocol with Collision Avoidance (802.11)

PROTOCOLS:

- IEEE 802.11 CSMA/CD (Wireless)
- IEEE 802.3 (Ethernet)
- IP/Ethernet (ICMP, UDP, TCP, ARP)
- Clear-channel mode for serial async multidrop protocols including: Modbus, DNP.3, Bisync, BSAP, DF1, TotalFlow, Poll Select

SECURITY

- Approved AP/Remotes list
- Failed login lockdown
- 900 MHz FHSS for *i*NET (DTS for *i*NET II)—provides inherent security from 802.11b devices
- Proprietary data framing
- 128-bit encryption
- Automatic rotating key algorithm

RADIO CHARACTERISTICS

GENERAL:

Frequency Range:	902–928 MHz ISM Band

Frequency Hopping Range:	Ten user-configurable 2.5 MHz-wide zones, each containing 8 frequencies
Hop Patterns:	8192, based on network name
Frequency Stability:	20 ppm

TRANSMITTER:

Power Output (at antenna connector):	MDS *i*NET: 0.1 to 1.0 watt (+20 dBm to +30 dBm) ±1.0 dB, *set by user*
	MDS *i*NET II: 0.1 to 741 mW (+20 to +29 dBm ±1.0 dB, *set by user*
Duty Cycle:	Continuous
Modulation Type:	Binary CPFSK
Output Impedance:	50 Ohms
Spurious:	–67 dBc
Occupied Bandwidth:	MDS *i*NET: 316.5 kHz MDS *i*NET II: 600 kHz

RECEIVER:

Type:	Double conversion superheterodyne
Sensitivity:	MDS *i*NET: –92 dBm @ 512 kbps < $1x10^{-6}$ BER
	MDS *i*NET: –99 dBm @ 256 kbps < $1x10^{-6}$ BER
	MDS *i*NET II: –95 dBm @ 1024 kbps < $1x10^{-6}$ BER
	MDS *i*NET II: –96 dBm @ 512 kbps < $1x10^{-6}$ BER
Intermodulation:	59 dB Minimum (EIA)
Desensitization:	70 dB
Spurious:	60 dB

RADIO CHARACTERISTICS

GENERAL:

Frequency Range:	902–928 MHz ISM Band
Frequency Hopping Range:	Ten user-configurable 2.5 MHz-wide zones, each containing 8 frequencies
Hop Pattern:	Based on network name
Frequency Stability:	20 ppm

TRANSMIT/RECEIVE RANGE

	MDS *i*NET–256 kbps	**MDS *i*NET II–512 kbps**
Fixed Range (typical):	10–15 miles	10-15 miles
Fixed Range (maximum):	15–25 miles	15-25 miles
Mobile Range (parked):	5–10 miles	
Mobile Range (moving):	2–3 miles	
	MDS *i*NET–512 kbps	**MDS *i*NET II–1024 kbps**
Fixed Range (typical):	5–10 miles	5-10 miles
Fixed Range (maximum):	10–15 miles	10-15 miles

Note: Specifications subject to change without notice or obligation.

NOTE: Range calculations for fixed locations assume a 6 dBd gain Omnidirectional antenna on a 100 ft tower at the AP, a 10 dBd gain Yagi on a 25 ft mast at the remote with output power decreased to yield maximum allowable EIRP (36 dBm), a 10 dB fade margin, and a mix of agricultural and commercial terrain with line of sight.

Range calculations for mobile units assume a 6 dBd gain Omni on a 100 ft tower at the AP, a 5 dBd gain Omni with 1 watt output power at 6 ft height, a 10 dB fade margin, and 90% confidence with near line-of-sight in a mix of agricultural and commercial terrain.

Actual performance is dependent on many factors including antenna height, blocked paths, and terrain.

6.4 CHANNEL HOP TABLE

The MDS *i*NET transceiver's hop table consists of 80 channels, numbered 0 to 79 as listed in Table 6-4. Center frequencies are calculated as follows (where Fn is the center frequency of channel n):

Fn = 902.5 MHz + n*316.5 kHz

The MDS *i*NET II transceiver operates on the same channel assignments, but because the modulation bandwidth is 600 kHz instead of 316.5 kHz it is recommended that the installer restrict channel usage to every other channel for units operating in the same area.

NOTE: Channels 24, 26, and 55 are not used.

Table 6-4. Channel Hop Table

Zone	Channel	Frequency
1	0	902.5000 *(iNET FHSS lowest channel)*
1	1	902.8165 *(iNET II DTS lowest channel)*
1	2	903.1330
1	3	903.4495
1	4	903.7660
1	5	904.0825
1	6	904.3990
1	7	904.7155
2	8	905.0320
2	9	905.3485
2	10	905.6650
2	11	905.9815
2	12	906.2980

Table 6-4. Channel Hop Table *(Continued)*

Zone	Channel	Frequency
2	13	906.6145
2	14	906.9310
2	15	907.2475
3	16	907.5640
3	17	907.8805
3	18	908.1970
3	19	908.5135
3	20	908.8300
3	21	909.1465
3	22	909.4630
3	23	909.7795
4	24	910.0960
4	25	910.4125
4	26	910.7290
4	27	911.0455
4	28	911.3620
4	29	911.6785
4	30	911.9950
4	31	912.3115
5	32	912.6280
5	33	912.9445
5	34	913.2610
5	35	913.5775
5	36	913.8940
5	37	914.2105
5	38	914.5270
5	39	914.8435
6	40	915.1600
6	41	915.4765
6	42	915.7930
6	43	916.1095
6	44	916.4260
6	45	916.7425
6	46	917.0590
6	47	917.3755
7	48	917.6920
7	49	918.0085
7	50	918.3250
7	51	918.6415
7	52	918.9580
7	53	919.2745
7	54	919.5910

Table 6-4. Channel Hop Table *(Continued)*

Zone	Channel	Frequency
7	55	919.9075
8	56	920.2240
8	57	920.5405
8	58	920.8570
8	59	921.1735
8	60	921.4900
8	61	921.8065
8	62	922.1230
8	63	922.4395
9	64	922.7560
9	65	923.0725
9	66	923.3890
9	67	923.7055
9	68	924.0220
9	69	924.3385
9	70	924.6550
9	71	924.9715
10	72	925.2880
10	73	925.6045
10	74	925.9210
10	75	926.2375
10	76	926.5540
10	77	926.8705
10	78	927.1870 *(iNET II DTS highest channel)*
10	79	927.5035 *(iNET FHSS highest channel)*

6.5 SNMP USAGE NOTES

6.5.1 Overview

The firmware release described in this manual contains major changes to the transceiver's SNMP Agent, several new MIB variables, and new Agent configuration options. This guide reviews the changes and shows how to properly configure the Agent to take advantage of these new features.

SNMPv3 Support

The updated SNMP Agent now supports SNMP version 3 (SNMPv3). The SNMPv3 protocol introduces Authentication (MD5/SHA-1), Encryption (DES), the USM User Table, and View-Based Access

(Refer to RFC2574 for full details). The SNMP Agent has limited SNMPv3 support in the following areas:

- Only MD5 Authentication is supported (no SHA-1). SNMPv3 provides support for MD5 and SHA-1. Currently, only MD5 Authentication is supported in the SNMP Agent.
- Limited USM User Table Manipulation. The SNMP Agent starts with 5 default accounts. New accounts can be added (SNMPv3 adds new accounts by cloning existing ones), but they will be volatile (will not survive a power-cycle).

  New views cannot be configured on the SNMP Agent. Views will be inherited for new accounts from the account that was cloned.

  The SNMP Agent uses one password pair (Authentication / Privacy) for all accounts. This means that when the passwords change for one user, they change for all users.

SNMPv3 Accounts

The following default accounts are available for the SNMP Agent:

enc_mdsadmin—Read/write account using Authentication and Encryption

auth_mdsadmin—Read/write account using Authentication

enc_mdsviewer—Read only account using Authentication and Encryption

auth_mdsviewer—Read only account using Authentication

def_mdsviewer—Read only account with no Authentication or Encryption

Context Names

The following Context Names are used (please refer to RFC2574 for full details):

Admin accounts: **context_a** / Viewer accounts: **context_v**

All accounts share the same default passwords:

Authentication default password: **MDSAuthPwd** / Privacy default password: **MDSPrivPwd**

Passwords can be changed either locally (via the console) or from an SNMP Manager, depending on how the Agent is configured. If passwords are configured and managed locally, they are non-volatile and will survive a power-cycle. If passwords are configured from an SNMP

manager, they will be reset to whatever has been stored for local management on power-cycle.

This behavior was chosen based on RFC specifications. The SNMP Manager and Agent don't exchange passwords, but actually exchange *keys* based on passwords. If the Manager changes the Agent's password the Agent doesn't know the new password; just the new key. In this case, only the Manager knows the new password. This could cause problems if the Manager loses the password. If that happens, the Agent becomes unmanageable. Resetting the Agent's passwords (and therefore keys) to what is stored in flash memory upon power-cycle prevents the serious problem of losing the Agent's passwords.

If passwords are managed locally, they can be changed on the Agent (via the console). Any attempts to change the passwords for the Agent via an SNMP Manager will fail when the Agent is in this mode. Locally defined passwords will survive a power-cycle.

In either case, the SNMP Manager needs to know the initial passwords that are being used in order to talk to the Agent. If the Agent's passwords are configured via the Manager, then they can be changed from the Manager. If the passwords are managed locally, then the Manager must be re-configured with any password changes in order to continue to talk to the Agent.

Password-Mode Management Changes

When the password management mode is changed, the active passwords used by the Agent may also change. Some common scenarios are discussed below:

Common Scenarios

- Passwords are currently being handled by the Manager. The assigned passwords are **Microwave** (Auth), and **Rochester** (Priv). Configuration is changed to manage the passwords locally. The passwords stored on the radio were Fairport (Auth), and Churchville (Priv) (If local passwords have *never* been used, then MDSAuthPwd and MDSPrivPwd will be used). These passwords will now be used by the Agent to re-generate keys. The Manager will need to know these passwords in order to talk to the Agent.
- Passwords are currently being managed locally. The local passwords are **Fairport** (Auth) and **Churchville** (Priv). Configuration is changed to handle the passwords from the Manager. The same passwords will continue to be used, but now the Manager can change them.
- Passwords are currently being managed locally. The local passwords are **Fairport** (Auth) and **Churchville** (Priv). Passwords are changed to **Brighton** (Auth) and **Perinton** (Priv). The Agent will immediately generate new keys based on these passwords and start using them. The Manager will have to be re-configured to use these new passwords.

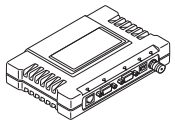
- Passwords are currently being managed locally. The local passwords are **Fairport** (Auth) and **Churchville** (Priv). Configuration is changed to handle the passwords from the Manager. The Manager changes the passwords to **Brighton** (Auth) and **Perinton** (Priv). The radio is then rebooted. After a power-cycle, the radio will use the passwords stored in flash, which are **Fairport** (Auth) and **Churchville** (Priv). The Manager will have to be re-configured to use these new passwords.

Table 6-5. SNMP Traps *(Sorted by Code)*

SNMP Trap	Severity	Description
systemBoot(32)	INFORM	SNR Within threshold/Below threshold
systemReboot(33)	MAJOR	Telnet User Logged Out/Logged In
startScan(34)	INFORM	Reprogramming Started
rxBeaconErrored(35)	INFORM	Received Beacon - Netname Does Not Match
rxBeaconWrongNetworkName (36)	INFORM	Received Beacon - AP is Blacklisted
rxBeaconFromBlacklistAP(37)	MAJOR	Max Beacon Wait Time Exceeded
expectedSync(38)	INFORM	Expected Sync Lost/Established
hopSync(39)	INFORM	Hop Sync Lost/Established
snr(41)	INFORM	Scanning Started
ber(42)	INFORM	Bit Error Rate Below threshold/Above threshold
associated(43)	MAJOR	Association Lost/Established
apParmChange(44)	MINOR	Association Lost - AP Hop Parameter Changed
reprogStarted(45)	MAJOR	Reprogramming Failed
reprogComplete(46)	MAJOR	Rem Ethernet Link Connected/Disconnected
reprogFailed(47)	INFORM	Reprogramming Complete
telnetLogin(48)	MAJOR	Telnet Access Locked for 5 Min
httpLogin(49)	MAJOR	HTTP User Logged Out/Logged In
countrySkipZoneMismatch(50)	INFORM	Country/SkipZone Mismatch
desiredAPIPMismatch(51)	INFORM	Desired AP IP Addr Mismatch
eventLogCleared(52)	INFORM	Log Cleared
authDemoMode(53)	MAJOR	Auth Demo Mode Expired -- Rebooted Radio/Enabled
keyEntered(54)	MAJOR	Auth Key Entered - Key Valid/Key Invalid
apEthLinkDown(55)	MAJOR	Association Lost - AP's Ethernet Link Down
noBeacons(56)	MAJOR	**MAC Param Changed**
apNotApproved(57)	MAJOR	Current AP No Longer Approved
netnameChanged(58)	MAJOR	Association Lost - Local Network Name Changed
ipAddrChanged(59)	MAJOR	Association Lost - Local IP Address Changed
assocTryFail(60)	MAJOR	Association Attempt Success/Failed
remEthLinkLost(61)	INFORM	Received Beacon - Valid/Errored
consoleLogin(62)	MAJOR	Console User Logged Out/Logged In

Table 6-5. SNMP Traps *(Sorted by Code)* ***(Continued)***

SNMP Trap	Severity	Description
consoleLockdown(63)	MAJOR	Console Access Locked for 5 Min
telnetLockdown(64)	INFORM	System Bootup (power on)
httpLockdown(65)	MAJOR	HTTP Access Locked for 5 Min
eventRemote(66)	INFORM	Remote added/removed from internal database
eventEndpoint(67)	INFORM	Endpoint added/removed from internal database
routeAdded(68)	INFORM	Radio attempted but failed to add a route to its internal routing table
routeDeleted(69)	INFORM	Radio attempted but failed to delete a route from its internal routing table
sinRemSwitch(70)	INFORM	Remote mode was switched (serial to ethernet, ethernet to serial)
chileChanCnt(71)	INFORM	Number of channels defined does not match (Chile only)
tftpConnection(73)	INFORM	TFTP Server on AP started or finished a transfer
apNetNameChanged(74)	MAJOR	Remote lost association due to a change in the AP's netname
ipConnectivityOK(75)	INFORM	Radio is associated AND 1) has an IP address statically defined, OR 2) received an IP address via DHCP
compressionChanged(76)	INFORM	Compression state has changed (enabled, disabled)
macDecryptError(77)	INFORM	MAC has received a packet that it could not decrypt
lanPortStatus(78)	INFORM	Ethernet port has changed (enabled, disabled)
tftpConnFailed(79)	INFORM	TFTP server on AP failed to transfer
sdbError(80)	INFORM	AP encountered an internal database error



7 GLOSSARY OF TERMS AND ABBREVIATIONS

If you are new to wireless IP/Ethernet systems, some of the terms used in this guide may be unfamiliar. The following glossary explains many of these terms and will prove helpful in understanding the operation of your radio network.

Access Point (AP)—The transceiver in the network that provides synchronization information to one or more associated Remote units. AP units may be configured for either the Access Point (master) or Remote services. (See *"Network Configuration Menu"* on Page 40.)

Active Scanning—See *Passive Scanning*

Antenna System Gain—A figure, normally expressed in dB, representing the power increase resulting from the use of a gain-type antenna. System losses (from the feedline and coaxial connectors, for example) are subtracted from this figure to calculate the total antenna system gain.

AP—See *Access Point*

Association—Condition in which the frequency hopping pattern of the Remote is synchronized with the Access Point station and is ready to pass traffic.

Authorization Key—Alphanumeric string (code) that is used to enable additional capabilities in the transceiver.

Bit—The smallest unit of digital data, often represented by a one or a zero. Eight bits (plus start, stop, and parity bits) usually comprise a byte.

Bits-per-second—See *BPS*.

BPDU—Bridge Protocol Data Units

BPS—Bits-per-second (bps). A measure of the information transfer rate of digital data across a communication channel.

Byte—A string of digital data usually made up of eight data bits and start, stop and parity bits.

CSMA/CA—Carrier Sense Multiple Access/Collision Avoidance

CSMA/CD—Carrier Sense Multiple Access/Collision Detection

Cyclic Redundancy Check (CRC)—A technique used to verify data integrity. It is based on an algorithm which generates a value derived

from the number and order of bits in a data string. This value is compared with a locally-generated value and a match indicates that the message is unchanged, and therefore valid.

Data Circuit-terminating Equipment—See *DCE*.

Data Communications Equipment—See *DCE*.

Datagram—A data string consisting of an IP header and the IP message within.

Data Terminal Equipment—See *DTE*.

dBi—Decibels referenced to an "ideal" isotropic radiator in free space. Frequently used to express antenna gain.

dBm—Decibels referenced to one milliwatt. An absolute unit used to measure signal power, as in transmitter power output, or received signal strength.

DCE—Data Circuit-terminating Equipment (or Data Communications Equipment). In data communications terminology, this is the "modem" side of a computer-to-modem connection. COM1 Port of the transceiver is set as DCE.

Decibel (dB)—A measure of the ratio between two signal levels. Frequently used to express the gain (or loss) of a system.

Delimiter—A flag that marks the beginning and end of a data packet.

Device Mode—The operating mode/role of a transceiver (Access Point or Remote) in a wireless network.

DHCP (Dynamic Host Configuration Protocol)—An Internet standard that allows a client (i.e. any computer or network device) to obtain an IP address from a server on the network. This allows network administrators to avoid the tedious process of manually configuring and managing IP addresses for a large number of users and devices. When a network device powers on, if it is configured to use DHCP, it will contact a DHCP server on the network and request an IP address.

The DHCP server will provide an address from a pool of addresses allocated by the network administrator. The network device may use this address on a "time lease" basis or indefinitely depending on the policy set by the network administrator. The DHCP server can restrict allocation of IP addresses based on security policies. An Access Point may be configured by the system administrator to act as a DHCP server if one is not available on the wired network.

Digital Signal Processing—See *DSP*.

DSP—Digital Signal Processing. DSP circuitry is responsible for the most critical real-time tasks; primarily modulation, demodulation, and servicing of the data port.

DTE—Data Terminal Equipment. A device that provides data in the form of digital signals at its output. Connects to the DCE device.

Encapsulation—Process in by which, a complete data packet, such as Modbus frame or any other polled asynchronous protocol frame, is placed in the data portion of another protocol frame (in this case IP) to be transported over a network. Typically this action is done at the receiving end, before being sent as an IP packet to a network. A similar reversed process is applied at the other end of the network extracting the data from the IP envelope, resulting in the original packet in the original protocol.

Endpoint—IP address of data equipment connected to the ports of the radio.

Equalization—The process of reducing the effects of amplitude, frequency or phase distortion with compensating networks.

Fade Margin—The greatest tolerable reduction in average received signal strength that will be anticipated under most conditions. Provides an allowance for reduced signal strength due to multipath, slight antenna movement or changing atmospheric losses. A fade margin of 15 to 20 dB is usually sufficient in most systems.

Fragmentation—A technique used for breaking a large message down into smaller parts so it can be accommodated by a less capable media.

Frame—A segment of data that adheres to a specific data protocol and contains definite start and end points. It provides a method of synchronizing transmissions.

Frequency Hopping—The spread spectrum technique used by the transceiver, where two or more associated radios change their operating frequencies several times per second using a set pattern. Since the pattern appears to jump around, it is said to “hop” from one frequency to another.

Frequency Zone—The radio uses up to 80 discrete channels in the 902 to 928 MHz spectrum. A group of 8 channels is referred to as a zone; in total there are 10 zones.

Hardware Flow Control—A transceiver feature used to prevent data buffer overruns when handling high-speed data from the connected data communications device. When the buffer approaches overflow, the radio drops the clear-to-send (CTS) line, that instructs the connected device to delay further transmission until CTS again returns to the high state.

Hop Pattern Seed—A user-selectable value to be added to the hop pattern formula in an unlikely event of nearly identical hop patterns of two collocated or nearby radio networks to eliminate adjacent-network interference.

Host Computer—The computer installed at the master station site, that controls the collection of data from one or more remote sites.

HTTP—Hypertext Transfer Protocol

IAPP (inter-Access Point Protocol)—A protocol by which access points share information about the stations that are connected to them. When a station connects to an access point, the access point updates its database. When a station leaves one access point and roams to another access point, the new access point tells the old access point, using IAPP, that the station has left and is now located on the new access point.

ICMP—Internet Control Message Protocol

IGMP (Internet Gateway Management Protocol)—Ethernet level protocol used by routers and similar devices to manage the distribution of multicast addresses in a network.

IEEE—Institute of Electrical and Electronic Engineers

Image (File)—Data file that contains the operating system and other essential resources for the basic operation of the radio's CPU.

LAN—Local Area Network

Latency—The delay (usually expressed in milliseconds) between when data is applied at the transmit port at one radio, until it appears at the receive port at the other radio.

MAS—Multiple Address System. A radio system where a central master station communicates with several remote stations for the purpose of gathering telemetry data. Figure 1-2 on Page 6 shows an example of an MAS system.

MAC—Media Access Controller

MCU—Microcontroller Unit. This is the processor responsible for controlling system start-up, synthesizer loading, hop timing, and key-up control.

MD5—A highly secure data encoding scheme. MD5 is a one-way hash algorithm that takes any length of data and produces a 128 bit "fingerprint." This fingerprint is "non-reversible," it is computationally infeasible to determine the file based on the fingerprint. For more details review "RFC 1321" available on the Internet.

MIB—Management Information Base

Microcontroller Unit—See *MCU*.

Mobile IP—An emerging standard by which access points and stations maintain network connectivity as the stations move between various IP networks. Through the use of Mobile IP a station can move from its home IP network to a foreign network while still sending and receiving data using it's original IP address. Other hosts on the network will not need to know that the station is no longer in its home network and can continue to send data to the IP address that was assigned to the station. Mobile IP also uses DHCP when the station moves into a foreign network.

Mobility—Refers to a station that moves about while maintaining active connections with the network. Mobility generally implies physical motion. The movement of the station is not limited to a specific network and IP subnet. In order for a station to be mobile it must establish and tear down connections with various access points as it moves through the access points' territory. To do this, the station employs roaming and Mobile IP.

Mode—*See Device Mode.*

MTBF—Mean-Time Between Failures

Multiple Address System (MAS)—See *Point-Multipoint System.*

Network Name—User-selectable alphanumeric string that is used to identify a group of radio units that form a communications network. The Access Point and all Remotes within a given system should have the same network address.

Network-Wide Diagnostics—An advanced method of controlling and interrogating MDS radios in a radio network.

NTP—Network Time Protocol

Packet—The basic unit of data carried on a link layer. On an IP network, this refers to an entire IP datagram or a fragment thereof.

Passive Scanning—Scanning is a process used by stations to detect other access points on network to which it may connect if it needs to roam. Passive scanning is a slower process in which it listens for information offered by the access points on a regular basis. Active scanning is a faster process in which the station sends out probe message to which the access points respond. Passive scanning can be done while maintaining the current network connectivity. Active scanning affects the RF configuration of the radio and therefore, at least temporarily, disconnects the station from the access point.

PING—Packet INternet Groper. Diagnostic message generally used to test reachability of a network device, either over a wired or wireless network.

Point-Multipoint System—A radio communications network or system designed with a central control station that exchanges data with a number of remote locations equipped with terminal equipment.

Poll—A request for data issued from the host computer (or master PLC) to a remote radio.

Portability—A station is considered connected when it has successfully authenticated and associated with an access point. A station is considered authenticated when it has agreed with the access point on the type of encryption that will be used for data packets traveling between them. The process of association causes a station to be bound to an access point and allows it to receive and transmit packets to and from the access point. In order for a station to be associated it must first authenticate with the access point. The authentication and association processes occur automatically without user intervention.

Portability refers to the ability of a station to connect to an access point from multiple locations without the need to reconfigure the network settings. For example, a remote transceiver that is connected to an access point may be turned off, moved to new site, turned back on, and, assuming the right information is entered, can immediately reconnect to the access point without user intervention.

PLC—Programmable Logic Controller. A dedicated microprocessor configured for a specific application with discrete inputs and outputs. It can serve as a host or as an RTU.

Remote—A transceiver in a network that communicates with an associated Access Point.

Remote Terminal Unit—See *RTU*.

RFI—Radio Frequency Interference

Roaming—A station's ability to automatically switch its wireless connection between various access points as the need arises. A station may roam from one access point to another because the signal strength or quality of the current access point has degraded below what another access point can provide. When two access points are co-located for redundancy, roaming allows the stations to switch between the access points to provide a robust network. Roaming may also be employed in conjunction with Portability where the station has been moved beyond the range of the original access point to which it was connected. As the station comes in range of a new access point, it will switch its connection to the stronger signal. Roaming refers to a station's logical, not nec-

essarily physical, move between access points within a specific network and IP subnet.

RSSI—Received Signal Strength Indicator

RTU—Remote Terminal Unit. A data collection device installed at a remote radio site.

SCADA—Supervisory Control And Data Acquisition. An overall term for the functions commonly provided through an MAS radio system.

Skip Zone(s)—Groups of operating channels (frequencies) deleted from the radio transmitter and receiver operating range.

SNMP—Simple Network Management Protocol

SNR—Signal-to-Noise Ratio. A measurement of the desired signal to ambient noise levels.This measurement provides a relative indication of signal quality. Because this is a relative number, higher signal-to-noise ratios indicate improved performance.

SNTP—Simple Network Time Protocol

SSL—Secure Socket Layer

STP—Spanning Tree Protocol

Standing-Wave Ratio—See *SWR*.

SWR—Standing-Wave Ratio. A parameter related to the ratio between forward transmitter power and the reflected power from the antenna system. As a general guideline, reflected power should not exceed 10% of the forward power (≈ 2:1 SWR).

TCP—Transmission Control Protocol

TFTP—Trivial File Transfer Protocol

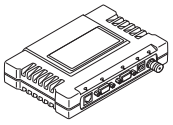
Trap Manager—Software that collects SNMP traps for display or logging of events.

UDP—User Datagram Protocol

UTP—Unshielded Twisted Pair

WINS—Windows Internet Naming Service. Part of Microsoft Windows NT and 2000 servers that manages the association of workstation names and locations with Internet Protocol addresses. It works without the user or an administrator having to be involved in each configuration change. Similar to DNS.

Zone—See *Frequency Zone*.



INDEX

Numerics

100BaseT 129
10BaseT 129
802.11b 8

A

Access Point (AP) 157
accessories 15
Active Scanning 161
Actual Data Rate 76
Add Associated Remotes 75
AgeTime 84, 85
alarm conditions 118
  correcting 120
Alarmed 116
Antenna
  aiming 125
  directional 136
  Minimum Feedline Length versus Antenna Gain 134
  omnidirectional 133
  polarization 132
  selection 132
  SWR check 124
  system gain 157
  system gain vs. power output setting 138
  Yagi 133
AP
  Auto Upgrade 84
  Reboot when Upgraded 84
application
  IP-to-Serial 67
  Mixed-Modes 72
  Point-to-Multipoint Serial-to-Serial 69
  Point-to-Point Serial-to-Serial 68
  Serial Port 72
Approved
  Access Points/Remotes List 74
  Remotes/Access Points List 75
Associated 116
Association 157
  Date 84
  Process 83
  Time 84
attenuation 20
Auth Traps Status 48
Authorization Key 105, 108, 157
Authorized Features 105
Auto Data Rate Menu
  RSSI Threshold/Delta 53
  SNR Threshold/Delta 53
Auto Key Rotation 74
Auto-Upgrade/Remote-Reboot 106

B

Backhaul
  for Serial Radio Networks 6
  Network 7
bandpass filter 136
Beacon
  Period 50, 90, 91
  signal 83
Begin Wizard 60
Bit 157
bits-per-second (bps) 157
BPDU 88, 157
BPS 157
Bridge Protocol Data Units 88, 157
byte 157
Bytes
  in on port 87
  in on socket 87
  out on port 87
  out on socket 87
  received 81, 82
  sent 81, 82

C

cable
  Ethernet crossover 20
  feedlines 133
  serial 20
Clear
  Com# statistics 87
  Ethernet stats 82
  Log 79
  Wireless stats 82
Collocating Multiple Radio Networks 13
Commit Changes and Exit Wizard 62, 63, 65, 66, 67
compression 49, 91
Computer
  host 160
configuration 21, 61, 63, 64, 66, 67
  basic device parameters 38
  defaults 21
  DHCP server 44
  editing files 104
  Ethernet Port 43
  file 97, 113

IP address 42
network 40
PPP Mode 66
radio parameters 48
scripts 97, 98
security 73
serial interfaces 56
SNMP Agent 46
TCP Mode 64
UDP mode 60
Connection Status 83
connectors 143
Contact 39
cost of deployment 8
Count 108
CRC (Cyclic Redundancy Check) 157
CSMA
CA 157
CD 157
Current
Alarms 79
AP IP Address 84
AP Mac Address 84
Custom Data Buffer Size 62, 63, 65, 66, 67
Cyclic Redundancy Check (CRC) 157

D

data
baud 67
baud rate 61, 63, 64, 66
buffering 59, 65
compression 91
rate 49
Data Terminal Equipment 159
Database
Logging 42
Timeout 42
Datagram 158
DataRate 85
Date 39
Format 39
dB 158
dBi 158
dBm 158
watts-volts conversion 139
DCE 158
decibel (dB) 158
default gateway 42
defaults
reset to factory 108
Delete
All Remotes 75
Remote 75
Delimiter 158
deployment costs 8
Description 39
Device
IP Address 67
Mode 36, 40, 41, 158
Name 36, 39
Status 36, 116
DHCP 42, 43, 158
Netmask 45
Server Configuration 41
Diagnostic Tools 118
Digital Signal Processing (DSP) 159
dimensions 129
DKEY command 124
DNS Address 45
DSP (Digital Signal Processing) 159
DTE 9, 57, 159
Dwell Time 50, 90
Dynamic Host Configuration Protocol 158
Dynamic Mode 43

E

EIA-232 9
Embedded Management System 21
Encapsulation 159
Encryption 74
Phrase 74
Ending Address 45
Endpoint 159
Listing 77
Listing Menu 85
ENI, MDS iNET 900 3
Equalization 159
Ethernet
Address 42
Link (H/W) Watch 44
Link Poll Address 44
Packet Statistics 82
port enabled/disabled 44
Rate Limit 44
Event Log 77, 78, 116, 118, 120, 121

F

Fade Margin 159
Feedline
selection 132, 133
Filename 80, 93, 97
firmware
installing 94
upgrade 93, 106
version 37, 38
Flow Control 59, 61, 63, 64, 66, 67
hardware 159
Force Key Rotation 74
Force Reboot 106
Fragmentation 159
Threshold 50, 88, 90
Frame 159
Frequency 107
hopping 159

zone 159
fuse replacement 145

G

gain
antenna 157
system 137
Glossary 157—163
Go 108

H

Hardware
flow control 159
Version 37, 38
Hop
Format 51
pattern 136
Pattern Seed 50, 160
Sync 116
Hopping
channels 149
frequency 159
pattern seed 160
Host computer 160
HTTP 160
Access 74
Security Mode 74
Hypertext Transfer Protocol 160

I

IANA 58
IAPP 160
ICMP 160
IEEE 160
IETF standard RFC1213 46
IGMP 160
Image
Copy 93
file 160
Verify 93
iNET II 50
iNET II, differences of 3, 4, 5, 14, 48, 49, 50, 51, 53, 54, 86, 125, 131, 135
Installation
antenna & feedline 132
feedline selection 133
general information 3
planning 129
requirements 129
site selection 131
site survey 135
Institute of Electrical and Electronic Engineers 160
Inter-Access Point Protocol 160
Interference 136
Internet
Assigned Numbers Authority 58
Control Message Protocol 160
IP 44
Addr 108
Address 36, 40, 84, 85, 104
address 43
Address Configuration 41
Address Mode 43
Gateway 104
Mobile 161
Protocol 61, 62, 64, 65, 67
tunneling 57

K

Key
authorization 157
transmitter, for antenna SWR check 124
KEY command 124

L

LAN 43, 160
Latency 90, 160
Latest AP Firmware Version 84
LED
COM1 23
COM2 23
LAN 23, 114
LINK 23, 24, 114, 126, 136
PWR 23, 78, 80, 114, 118, 121
use during troubleshooting 113
Link Established 67
Local
Area Network 160
IP Port 61, 62
Listening IP Port 65
Location 39, 104
Logged Events 121
Lost Carrier Detected 82, 117

M

MAC Address 84, 85, 88
Management Information Base 160
Management System 21
user interfaces 27
MAS 160
Master Station 160
Maximum Remotes 41
MCU (Microcontroller Unit) 160
MD5 160
MDS iNET 900 ENI 3
MDS Security Suite 14
SNMP traps 15
Mean-Time Between Failures 161
measurements

radio 123
MIB 160
files 46
Microcontroller Unit 160
Mobile 54
Mobile Data
Beacon Period 56
Compression 55
configuration 54
Dwell Time 56
Fragmentation Threshold 56
RTS Threshold 56
Mobile IP 161
Mobility 161
Mobility Capability 10
MODBUS 65
Mode
Device 158
mixed 71
serial gateway interface 10
TCP 10
UDP 10
Model Number 38
MTBF 161
Multicast
IP Address 61
IP Port 61
multiple
protocols 7
services 7
Multiple Address System (MAS) 160

N

NEMA 8
net mask 42
NETview MS 105
Network
Name 13, 19, 36, 40, 41, 104, 161
Time Protocol (NTP) 161
-wide diagnostics 161
network
bridge 87
maintenance 91
operation principles 87
performance optimization 90
performance verification 76
network design 10
antennas 11
collocating multiple radio networks 13
network name 11
repeaters 10
using multiple Access Points 12
Using the AP as a Store-and-Forward Packet Repeater 12
using two transceivers to form a repeater station 10
NTP (Network Time Protocol) 161

O

Outgoing Connection□s Inactivity Timeout 64
Owner 39

P

Packet 161
Redundancy Mode 61, 63
Size 108
Statistics 77, 81, 117
Packets
Dropped 81, 82, 117
Received 81, 82
Received by Zone 82
Sent 81, 82
Passive Scanning 161
password
resetting 108
PC
connection to transceiver 20
Performance Information Menu 90
PING 19, 24, 135, 162
Ping Utility 108
PLC 8, 162
Point-Multipoint System 162
Point-to-Point
LAN Extension 6
Link 6
Poll 162
port
antenna 124
COM1 9, 20, 21, 22, 57, 68, 132, 144
COM2 9, 22, 57, 68, 144
Ethernet 19
IP 68
LAN 21, 22, 143
not Enabled 67
Portability 162
ports
serial 7
power
how much can be used 135
primary 20
transmitter power output 124
PPP 59
Primary Host Address 64
Primary IP Port 64
Programmable Logic Controller 8
protocol
BPDU 88
HTTP 160
IAPP 160
ICMP 160
IP 22, 44, 56
MODBUS 65
PPP 59
SNMP 27, 46, 151, 163

SNTP 41, 163
STP 88, 163
TCP 57, 58, 64, 67, 71, 90, 163
TFTP 94, 163
UDP 57, 58, 67, 68, 71, 90, 163

R

Radio
Frequency Interference 13, 136
Remote 162
Test 107
range, transmission 8
Read Community String 47
Reboot
Device 93
on Upgrade 106
Receive errors 81, 82, 117
Received Signal Strength Indicator 20, 131, 163
Redundancy
Using multiple Access Points 12
Remote
IP Address 62
IP Port 62
Listing 77
Listing Menu 84
Performance Listing 77, 86
radio 162
Terminal Unit 8, 163
Repeater 10
antennas 11
Network Name 11
Using the AP as a Store-and-Forward Packet Repeater 12
Using two transceivers to form a repeater station 10
reprogramming 92
Restart DHCP Server 45
Retries 82, 117
Retrieve File 93, 97
Retry errors 82, 117
RetryEr 86
RF Output Power 49, 76
RFI 13, 162
Roaming 162
RSSI 20, 76, 108, 117, 125, 131, 163
by Zone 76, 77
Threshold 51
RTS Threshold 50, 88, 90
RTS/CTS handshaking 61
RTU 8, 57, 68, 72, 163
RxBCMC 86
RxPkts 85, 86
RxRate 86
RxViaEP 86

S

Save Changes 75
SCADA 7, 8, 58, 163
Scanning 116
Active 161
Passive 161
Seamless Inter-Frame Delay 61, 63, 65, 66, 67
Secondary
Host Address 64
IP Port 64
Secure Socket Layer 163
security
Approved Access Points/Remotes List 74
Auto Key Rotation 74
encryption 74
Encryption Phrase 74
Force Key Rotation 74
general information 3
HTTP Access 74
HTTP Security Mode 74
risks 14
SNMP Access 74
suite 14
Telnet Access 74
Two-Way Authentication 73
User Password 74
security suite
SNMP traps 15
Send
File 97
Log 79
Sending LCP Requests 67
Serial
Configuration Wizard 59
Data Statistics 87
encapsulation 57
Mode 61, 63, 65, 66, 67
Number 37, 38
Port Statistics 117
radio networks, backhaul 6
Server Status 45
Signal strength 131
Signal-to-Noise Ratio 76, 163
Simple Network
Management Protocol 163
Time Protocol 163
Site selection 131
Skip Zone 163
SNMP 27, 163
Access 74
Config Menu 41
Mode 47
traps 15, 154
usage 151
V3 Passwords 48
SNR 51, 163
Threshold 51
SNTP 41, 163
Spanning Tree Protocol 88, 163
Specifications 146—149
SSL 163
Standing Wave Ratio 163

Starting
Address 45
Information Screen 37
State 84
Static IP
Address 43
Gateway 43
Netmask 43
Status 36, 60, 62, 64, 65, 67
STP 163
subnet 43
Supervisory Control and Data Acquisition (SCADA) 163
SWR 124, 163
performance optimization 124
Syslog Server 80
system gain, antenna 157
System Mode 104

T

TCP 10, 58, 71, 90, 163
Client 58
Server 58
Telnet 68
Access 74
Test Mode 107
TFTP 163
Host Address 79, 93, 97
Time-out 80
Timeout 93, 97
Time 39
Time to Live (TTL) 61
Transmission
Control Protocol 163
range 8
transparent encapsulation 57
Trap
Community String 47
Manager 48, 163
Version 48
Trivial File Transfer Protocol 163
Troubleshooting 113—123
Using the Embedded Management System 114
Two-Way Authentication 73
TX Output Power 107
TxKey 108
TxPkt 86
TxPkts 86
TxViaEP 86

U

UDP 10, 58, 68, 71, 90, 163
mode 60
Unit Name 104
Unshielded Twisted Pair 163
Uptime 37, 39
User Datagram Protocol 163
User Password 74
Using multiple Access Points 12
UTP 163

V

V3
Authentication Password 47
Privacy Password 47
via Remote 85
View
Approved Remotes 75
Current Alarms 80
Current Settings 60
Event Log 81
Log 79
volts-dBm-watts conversion 139

W

watts-dBm-volts conversion 139
WINS 163
Address 45
Wireless
Address 42
Network Status 77, 83
Packet Statistics 81
wizard
serial configuration 59
Write community String 47

Y

Yagi antenna 133

IN CASE OF DIFFICULTY...

MDS products are designed for long life and trouble-free operation. However, this equipment, as with all electronic equipment, may have an occasional component failure. The following information will assist you in the event that servicing becomes necessary.

TECHNICAL ASSISTANCE

Technical assistance for MDS products is available from our Technical Support Department during business hours (8:00 A.M.—5:30 P.M. Eastern Time). When calling, please give the complete model number of the radio, along with a description of the trouble/symptom(s) that you are experiencing. In many cases, problems can be resolved over the telephone, without the need for returning the unit to the factory. Please use one of the following means for product assistance:

Phone: 585 241-5510 E-Mail: TechSupport@microwavedata.com

FAX: 585 242-8369 Web: www.microwavedata.com

FACTORY SERVICE

Component level repair of radio equipment is not recommended in the field. Many components are installed using surface mount technology, which requires specialized training and equipment for proper servicing. For this reason, the equipment should be returned to the factory for any PC board repairs. The factory is best equipped to diagnose, repair and align your radio to its proper operating specifications.

If return of the equipment is necessary, you will be issued a Service Request Order (SRO) number. The SRO number will help expedite the repair so that the equipment can be repaired and returned to you as quickly as possible. Please be sure to include the SRO number on the outside of the shipping box, and on any correspondence relating to the repair. No equipment will be accepted for repair without an SRO number.

A statement should accompany the radio describing, in detail, the trouble symptom(s), and a description of any associated equipment normally connected to the radio. It is also important to include the name and telephone number of a person in your organization who can be contacted if additional information is required.

The radio must be properly packed for return to the factory. The original shipping container and packaging materials should be used whenever possible. All factory returns should be addressed to:

Microwave Data Systems
Product Services Department
(SRO No. XXXX)
175 Science Parkway
Rochester, NY 14620 USA

When repairs have been completed, the equipment will be returned to you by the same shipping method used to send it to the factory. Please specify if you wish to make different shipping arrangements. To inquire about an in-process repair, you may contact our Product Services Group at 585-241-5540 (FAX: 585-242-8400), or via e-mail at ProductServices@microwavedata.com.

industrial/wireless/performance

Microwave Data Systems Inc.
175 Science Parkway
Rochester, NY 14620
General Business: +1 585 242-9600
FAX: +1 585 242-9620
Web: www.microwavedata.com

A product of Microwave Data Systems Inc.